

# Schlussbericht des SumoDacs-Konsortiums

## SumoDacs: Secure Mobile Data Access



*Förderkennzeichen:*

01IS09035A, 01IS09035B, 01IS09035C

*Laufzeit des Vorhabens:*

01.11.2009 – 31.10.2011

GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung

*Zuwendungsgeber:*

**Bundesministerium für Bildung und Forschung**

*Zuwendungsempfänger:*

**CAS Software AG, Karlsruher Institut für Technologie (KIT), WIBU-SYSTEMS AG**



*Ort, Datum*

**Karlsruhe, 4. Mai 2012**

## Inhalt

**ABBILDUNGSVERZEICHNIS II****TABELLENVERZEICHNIS II**

<b>I. SCHLUSSBERICHT (I)</b>	<b>3</b>
1 Aufgabenstellung und Projekthintergrund .....	3
1.1 Funktionalitäten von SumoDacs	3
1.2 Lösungsansatz	5
2 Ausgangslage und Voraussetzungen.....	6
2.1 Hardware-Token in SumoDacs	7
3 Planung und Ablauf des Vorhabens.....	9
4 Wissenschaftlicher und technischer Stand.....	16
4.1 Technischer Stand und Konkurrenzprodukte	16
5 Zusammenarbeit mit anderen Stellen .....	18
<b>II. SCHLUSSBERICHT (II), EINGEHENDE DARSTELLUNG</b>	<b>19</b>
1 Erzielte Ergebnisse .....	19
2 Arbeitspakete .....	21
2.1 Anforderungsanalyse	21
2.2 Bedrohungsanalyse	22
2.3 Entwurf der Gesamtarchitektur	23
2.4 Kryptographische Protokolle	28
2.5 Datenmodell für Zugriffskontrolle	29
2.6 Backend-Integration	34
2.7 Integration Hardware-Token	34
2.8 Implementierung mobile Clients	36
2.9 Vorgehensmodell	39
2.10 Wissenschaftliche Evaluation	44
3 Notwendigkeit und Angemessenheit der geleisteten Arbeiten .....	47
4 Verwertbarkeit der Ergebnisse.....	47
5 Fortschritte auf dem Gebiet des Vorhabens .....	50
6 Erfolgte und geplante Veröffentlichungen.....	51

## Abbildungsverzeichnis

Abbildung 1: Überblick Architektur von SumoDacs	5
Abbildung 2: Aktuelle CodeMeter Hardware-Token	9
Abbildung 3: Firewalls und SumoDacs Sicherheitsserver, 3-Zonen Modell	24
Abbildung 4: Übersicht nPA-Demonstrator	25
Abbildung 5: Einbindung der Hardware-Token	27
Abbildung 6 Backend-Integration mit cas open	28
Abbildung 7: Berechtigungsmodell mit Kontext-Schaltern	32
Abbildung 8: Prinzip "Kontext-Schalter"	33
Abbildung 9: Screenshot Identitätsnachweis mit nPA	35
Abbildung 10: Screenshot des nPA-Demonstrators, nPA und Lizenzaktivierung mit LicenseCentral	35
Abbildung 11: Übersicht nPA-Demonstrator, Reverse Proxy (http-Proxy)	36
Abbildung 12: Webbasierter stationärer/mobiler Client: AusweisApp, Browser und http-Proxy zur Unterstützung von nPA und CodeMeterAct sowie von CodeMeter-Token (Stick und microSD)	37
Abbildung 13: Gesamtvorgehensmodell.	40
Abbildung 14: Teilvorgehensmodell Berechtigung	41
Abbildung 15: Teilmodell Backend Integration.	42
Abbildung 16: Teilmodell Mobile Client Implementierung.	42
Abbildung 17: Handhabung des Token mit PC / TabletPC im Vergleich zum Zurechtfinden in der Anwendung	45
Abbildung 18: Vergleich der Szenarien-Tage bzgl. Einfachheit	46
Abbildung 19 - Weiterentwicklung von CAS Open zu einer ‚Platform as a Service‘ und Marktein-führung	48

## Tabellenverzeichnis

Tabelle 1: Übersicht Arbeitspakete	10
Tabelle 2: Übersicht über die Arbeitspakete	15
Tabelle 3: Meilensteine	15

## **I. SCHLUSSBERICHT (I)**

### **1 AUFGABENSTELLUNG UND PROJEKTHINTERGRUND**

Ziel des Projekts SumoDacs ist die Entwicklung einer Architektur für den sicheren Zugriff auf Unternehmensdaten mit mobilen Endgeräten unter Verwendung von Hardware-Tokens. Die Hardware steht bereits in für mobile Anwendungen geeigneten Bauformen zur Verfügung, z.B. als USB-Stick oder als SD-Card; zusätzlich wird auch der zukünftige elektronische Personalausweis (nPA) als Token verwendet. Ein kontextsensitives Berechtigungssystem wird eine flexible und feingranulare Zugriffskontrolle sowie digitales Rechtemanagement ermöglichen, welche die Herausforderungen ubiquitärer Anwendungsszenarien erfüllt.

Nach Abschluss des Projekts steht eine prototypische Referenzlösung zur Verfügung, die im CRM-System von CAS eine browserbasierte Sicherheitslösung für Clients bietet. Die Prototyplösung wird zeitnah nach Abschluss des Projekts zu verschiedenen Produkten zum sicheren Zugang, d.h. Access- und Identity Management und zum Schutz von Anwenderdaten weiterentwickelt und angeboten. WIBU-SYSTEMS bietet Entwicklungstools an, um mobile Sicherheitsanwendungen einfach zu integrieren. Dadurch wird ein neues Marktpotential für den Schutz und die Lizenzierung digitaler Produkte erschlossen. Dies wiederum generiert weiteres wirtschaftliches und beschäftigungsmäßiges Wachstum.

#### **1.1 FUNKTIONALITÄTEN VON SUMODACS**

SumoDacs soll folgende Funktionalitäten bieten:

- Über Security-Token abgesicherter Zugriff mit mobilen Endgerät (z.B. Smartphone) auf einem stationären Backend-Server gespeicherte Daten (z.B. CRM-Daten, ERP-Daten, PIM-Daten, Dokumente).
- Über Security-Token abgesicherter Zugriff mit nicht vertrauenswürdigen stationärem Desktop-PC (z.B. Terminal in Hotel/Internet-Cafe, Gastrechner in Firma) auf Backend-Daten.
- Als Security-Token kann auch der elektronische Personalausweis, der im Jahre 2010 in Deutschland eingeführt wurde [Bitk09, Seite 63]<sup>1</sup>, verwendet werden. Hierzu ist ein NFC-fähiges Endgerät notwendig.
- Kontextabhängige dynamische Rollen: Berechtigungen für die Ausübung bestimmter Operationen auf vom System verwaltete Ressourcen sind an Rollen gebunden. Diese Rollen können in Abhängigkeit von Kontextparametern (z.B. Art der Authentifizierung, Ort, Verschlüsselung der Datenkommunikation) aktiviert und deaktiviert werden; bestimmte Rollen können sich auch gegenseitig ausschließen.

---

<sup>1</sup> [Bitk09] BITKOM: Wachstumskräfte stärken. Die Hightech Agendafür die 17. Wahlperiode, Berlin 2009, [http://bitkom.org/files/documents/BITKOM-Hightech-Agenda\\_2009.pdf](http://bitkom.org/files/documents/BITKOM-Hightech-Agenda_2009.pdf).

- Abfangen von Verbindungsabbrüchen durch das sichere Zwischenspeichern von Daten, entweder durch das Hardware Security Token verschlüsselt auf dem Endgerät oder im Token selbst.
- Mandantenfähigkeit im Sinne der „Chinese-Wall-Security-Policy“ [BrNa89]<sup>2</sup>: wenn ein Nutzer einmal auf bestimmte Daten zugegriffen hat, kann automatisch der Zugriff auf andere Daten untersagt werden. Hierdurch wird eine Mandantenfähigkeit erreicht.
- Wipe-Out-Funktion, um sensible Daten auf verlorenen oder gestohlenen Endgeräten zu löschen, z.B. durch Steuernachricht beim nächsten Einbuchten des Gerätes (Remote-Wipe-Out, „Kill-Pill“), wenn Authentifizierung für einen bestimmten Zeitdauer nicht durchgeführt wird (Auto-Wipe-Out) oder wenn das Gerät einen bestimmten Bereich verlässt (Geo-Fencing).

Der Sicherheitsserver als Mediator zwischen den mobilen Endgeräten und den Unternehmensanwendungen verfügt über folgende Kernfunktionen:

- Authentifizierung: bevor ein Client auf Daten über SumoDacs zugreifen kann, muss er erst seine Identität nachweisen. In herkömmlichen Systemen geschieht dies durch Eingabe von Nutzernamen und Passwort. Bei SumoDacs ist hierzu auch der Besitz eines Hardware-Tokens notwendig.
- Policy-Komponente: Welche Zugriffsoperation (z.B. lesen, schreiben) ein Nutzer auf welchen Daten durchführen darf wird durch ein Rollenmodell festgelegt. Dieses Rollenmodell berücksichtigt insbesondere auch Kontextparameter bei der Entscheidung, ob ein Nutzer einen bestimmten Zugriff durchführen darf oder nicht.
- Verschlüsselung: Die Daten werden für den Transport zwischen dem Sicherheitsserver und dem Client verschlüsselt; diese Komponente verschlüsselt daher ausgehende Daten und entschlüsselt eingehende Daten.
- Datensynchronisation und Store&Forward: eine besondere Herausforderung bei Verwendung drahtloser Datenkommunikation ist die Berücksichtigung von ungeplanten Kommunikationsabbrüchen (z.B. „Funkloch“). Die SumoDacs-Architektur sieht deshalb vor, dass mobile Endgeräte auch teilweise autark arbeiten können, also einen eigenen Datenbestand vorhalten. Zum Abgleich dieses Datenbestandes wird eine Synchronisationskomponente benötigt. Auf einem mobilen Endgerät vorgehaltene Daten können auch verschlüsselt werden, damit beim Verlust des Endgerätes die Daten nicht Unbefugten in die Hände fallen. Falls eine Unternehmensanwendung eine Nachricht an einen mobilen Client schicken möchte, während dieser gerade keine Verbindung hat, wird diese Nachricht in der Store-&-Forward-Komponente zwischengespeichert, bis sie ausgeliefert werden kann.

---

<sup>2</sup> [BrNa89] D. F. C. Brewer, M. J. Nash: The Chinese Wall Security Policy. Proceedings of the IEEE Symposium on Research in Security and Privacy, 1989, 206-214.

## 1.2 LÖSUNGSANSATZ

Im Rahmen des Vorhabens soll eine verteilte Software-Architektur entwickelt werden, die den sicheren mobilen Zugriff auf beliebige „stationäre“ Datenbestände und Systeme ermöglicht. Hierzu müssen sowohl Software-Komponenten für stationäre Systeme (zentraler Sicherheitsserver, Integrations-Wrapper, Konfigurations-Tool) als auch Komponenten (Client-Software) für verschiedene mobile Endgeräteplattformen entwickelt werden. Da ein wichtiger Bestandteil des Sicherheitskonzepts ein Hardware-Security-Token ist, müssen zur Kommunikation zwischen diesem und den mobilen Endgeräten entsprechende Software-Komponenten entwickelt werden. Solche Software-Komponenten sind auch für die NFC-basierte Kommunikation mit dem elektronischen Personalausweis als Security-Token notwendig. Ein weiteres besonderes Merkmal von SumoDacs ist das auf kontextsensitiven Rollen basierende flexible Zugriffskonzept, das die Formulierung mobilspezifischer Berechtigungsregeln ermöglicht.

Der Lösungsansatz von SumoDacs lässt sich am besten anhand der in Abbildung 1 dargestellten Gesamtarchitektur erklären: Die beiden vertikalen Firewall-Grenzen unterteilen die Grafik in drei Zonen: die erste Zone (von links) stellt das interne sichere Netzwerk des Unternehmens dar; die zweite Zone ist die durch eine innere und äußere Firewall abgegrenzte demilitarisierte Zone (DMZ). Sie dient als Schutzzone zwischen dem internen Netzwerk und der dritten Zone, dem öffentlichen und damit nicht vertrauenswürdigen drahtlosen und drahtgebundenen Internet.

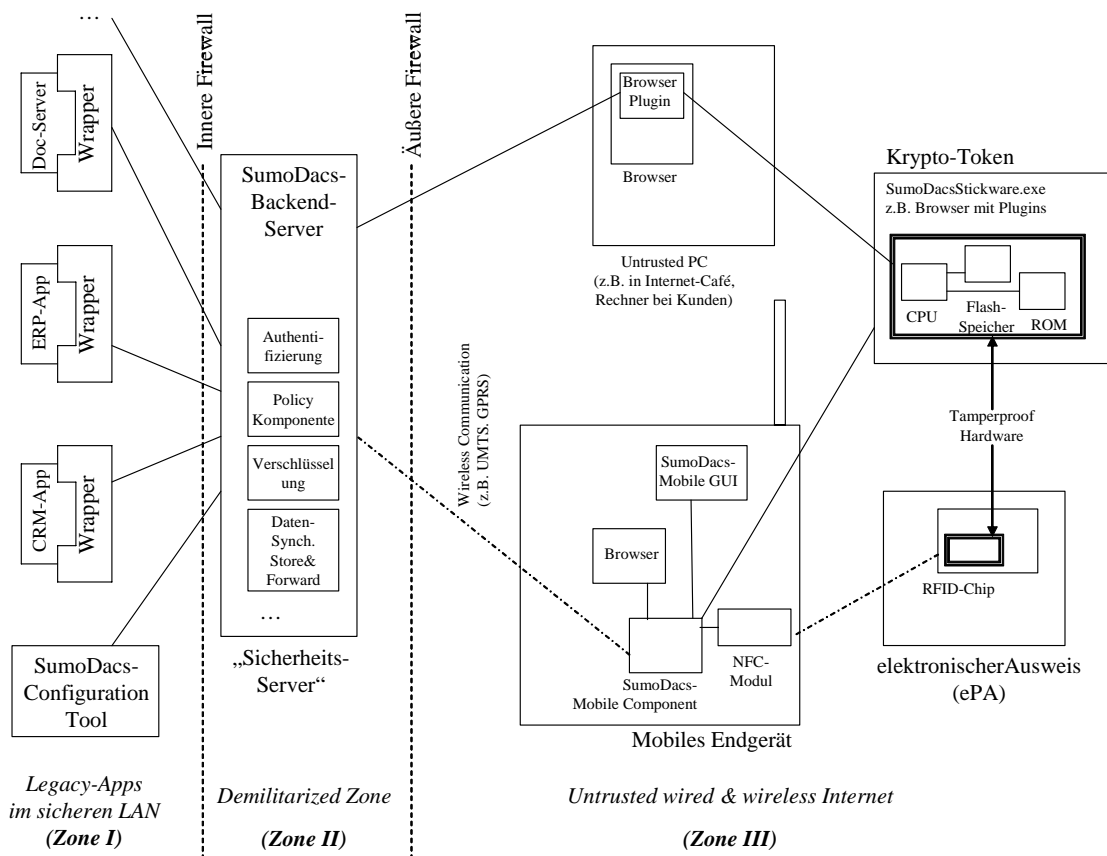


Abbildung 1: Überblick Architektur von SumoDacs

**Zone I** umfasst die Server mit den Unternehmensanwendungen (z.B. ERP, Dokumentenmanagement, CRM, Datenbanken), auf die ein sicherer Zugriff mit mobilen Endgeräten ermöglicht werden soll. Hierzu werden die einzelnen Anwendungsserver der Unternehmensanwendungen (Legacy-Anwendungen) durch auf die jeweiligen Protokolle und Schnittstellen angepassten Wrapper gekapselt.

In **Zone II** befindet sich der SumoDacs-Backend-Server („Sicherheits-Server“). Alle Kommunikationsverbindungen zwischen mobilen Clients aus Zone III und den Applikationen in Zone I müssen über ihn laufen. Die Kernfunktionen des Servers (Authentifizierung, Policy-Komponente, Verschlüsselung, Datensynchronisation, Store & Forward) werden im nächsten Unterkapitel eingehender beschrieben. Da der Sicherheitsserver modular aufgebaut ist, können weitere Funktionalitäten bei Bedarf einfach entwickelt und nachgerüstet werden. Für die Administration des Sicherheitsservers steht ein spezielles Administrationstool zur Verfügung, das in Zone I betrieben wird.

**Zone III** ist das ungesicherte öffentliche Internet, über das die Außendienstmitarbeiter mit ihren mobilen Endgeräten auf die Unternehmensdaten zugreifen. Es werden zwei Arten von Clients unterschieden: mobile Clients (also Endgeräte wie Notebooks, Netbooks, PDAs, Smartphones), die über drahtlose Datenkommunikation (z.B. GPRS, UMTS, EDGE) mit dem Sicherheitsserver verbunden sind; es sind aber auch stationäre Clients vorgesehen (also Desktop-PCs), wobei diese als nicht vertrauenswürdige Endgeräte betrachtet werden, z.B. Rechner in Internet-Cafés, Hotels, bei Kunden oder Privatrechner. Zusätzlich zum Endgerät ist auch der Besitz eines Hardware-Tokens notwendig; es handelt sich hierbei um ein gegen Manipulationsversuche geschütztes Smartcard-Modul in einer zu gängigen mobilen Endgeräten kompatiblen Form, z.B. als USB-Stick oder (μ)SD-Karte. Dieses Token kapselt kryptografische Schlüssel und ggf. weitere Informationen, die nicht ausgelesen werden

## **2     AUSGANGSLAGE UND VORAUSSETZUNGEN**

Das Marktumfeld im mobilen Bereich entwickelt sich sehr dynamisch, seitdem Endgeräte der neueren Mobilfunkgeneration Internetfähigkeit für den Massenmarkt anbieten und der Markt für mobile Datenkommunikation explosionsartig wächst. Hinzu kommen UMTS-Sticks für Laptop-Datenanwendungen sowie der Trend zur Integration von 4G-Datenmodems in Netbooks, Tablets und Smartphones. Dies sind die Voraussetzungen, die insgesamt die mobilen Webanbindungen für einen breiten Anwendermarkt interessant machen. Das hohe Datenvolumen wird nicht mehr alleine durch professionelle Anwender generiert, sondern auch durch das Bedürfnis der Consumer nach dem Zugang zu allen möglichen Arten von Informations- und Entertainment-Anwendungen. Es kann davon ausgegangen werden, dass die mobile Datenkommunikation bei anhaltend starkem Wachstum neben der klassischen Telefonie ein Hauptumsatzträger für die Mobilfunkbetreiber werden wird. Mobile Datenübertragungsraten von bis zu theoretischen 100 MBits/sec sind bereits für das Jahr 2012 angekündigt. "Software as a Service" ist daher mit zunehmender Verfügbarkeit von Breitbandkommunikation auch mobil ein starker Trend, der sich über alle Netzinfrastrukturen erstrecken wird. Security ist dabei eine essentielle Voraussetzung, so dass sich vertrauenswürdige Webservices auf offenen Plattformen weiter entwickeln können.

SumoDacs-Komponenten sind weitgehend plattformunabhängig und sollen über „Software as a Service“ überall installierbar und lauffähig sein. Das SumoDacs-Konzept versteht sich als offene und

dabei doch sichere mobile Lösung, die sowohl Software als auch Daten und Content absichern kann. Mit dieser Architektur lassen sich mobile Enterprise und e-Commerce-Anwendungen schnell verbreiten.

## **2.1 HARDWARE-TOKEN IN SUMODACS**

Das sichere Hardware-Token ist ein wesentlicher Bestandteil in der Lösung von SumoDacs. Es speichert kryptografische Schlüssel und weitere Informationen, die nicht ausgelesen werden können. Darüber hinaus ist es resistent gegen speziellen Angriffe auf die Hardware, beispielsweise:

- Auslesen unter Elektronenmikroskop
- Side-Channel-Angriffe wie Differential Power Analysis
- unerlaubte Betriebsbedingungen oder gezielte Störungen durch Lichtpulse.

Eine hundertprozentige Sicherheit gibt es auch bei sicherer Hardware nicht, allerdings sind erfolgreiche Angriffe nur mit sehr hohem Aufwand möglich und können in der Regel nur von Spezialisten mit entsprechendem Know-how und aufwändiger Messtechnik durchgeführt werden, beispielsweise im DPA-Labor von Giesecke & Devrient oder mit Messtechnik von escrypt in Bochum.

Mit „Common Criteria“, CC, liegt neben ITSEC ein internationales Kriterienwerk für die Sicherheitsbewertung vor. Die CC entstand in intensiver Zusammenarbeit europäischer Länder mit Vertretern der USA und Kanada. Die EAL-Stufen der Common Criteria (ISO 15408) beschreiben präzise Anforderungen der IT-Sicherheitsprüfung, deren Anforderungen mit wachsender EAL-Nummer steigen. Eine detaillierte Beschreibung der Sicherheitsleistung eines zertifizierten Produkts kann im Zertifizierungsreport nachgelesen werden (<http://www.commoncriteriaportal.org>). Weitere Informationen zu Common Criteria sind auf der Webseite des Bundesamts für Sicherheit in der Informationstechnik, <http://www.bsi.bund.de> zu finden.

Die eingesetzten Hardwaretoken enthalten ausnahmslos Sicherheitscontroller oder Smart Card Chips, die Common Criteria EAL 4 hoch zertifiziert wurden.

Weiterhin bieten die Token folgende Funktionen:

- Ver- und Entschlüsseln von Daten mit symmetrischen oder asymmetrischen Verfahren
- Erzeugung digitaler Signaturen
- Umfangreiches Rechtemanagement für Daten unterschiedlicher Rechteinhaber
- Sichere Speicherung von Daten und ausführbaren Programmen

Die verschiedenen Bauformen (z.B. USB-Stick, SD-Karte) stehen bereits zur Verfügung und sollen nicht im Rahmen des Projektes entwickelt werden; es ist aber denkbar, das in der Projektlaufzeit weitere Bauformen von WIBU-SYSTEMS als Reaktion auf aktuelle Marktentwicklungen bereitgestellt werden; die Hardware-Entwicklung dieser neuen Bauformen wäre aber nicht Gegenstand von SumoDacs, sondern nur die daraus resultierende softwaremäßige Integration.



Die Abbildung 2 zeigt die Hardware-Token, die zum Einsatz kamen. Es sind im Einzelnen folgende CodeMeter Produkte von WIBU-SYSTEMS (von links nach rechts):

- CmStick: Smart Card basierter USB-Token mit Samsung SmartCard Chip aus der Serie S3FS9CI mit 768 kByte Flash-Speicher und 32 Bit Secure-ARM-Prozessor, Common-Criteria [WIBU03]<sup>3</sup> zertifiziert EAL 4+, seit 2003 in einer ersten Version verfügbar, seit 2008 mit Samsung Chip
- CmStick/M: Smart Card basierter USB-Token mit zusätzlichem Flash-Massenspeicher, auf dem Programme und Daten gespeichert werden können, mit Atmel SmartCard Chip AT90SC7272C mit 8 Bit RISC Controller und zusätzlichem 16 Bit Crypto Controller, Common-Criteria [WIBU03] zertifiziert EAL 4+, seit 2004 verfügbar
- CmCard/M, CmCard/E: Smart Card basierter Token in einer PCCard (PCMCIA) oder ExpressCard|34 mit zusätzlichem Flash-Massenspeicher, auf dem Programme und Daten gespeichert werden können, mit Atmel SmartCard Chip AT90SC7272C mit 8 Bit RISC Controller und zusätzlichem 16 Bit Crypto Controller, Common-Criteria [WIBU03] zertifiziert EAL 4+, seit 2004 verfügbar
- CmCard/CF: Smart Card basierte Compact Flash-Karte (CF Card) mit Samsung SmartCard Chip aus der Serie S3FS9CI mit zusätzlichem Flash-Massenspeicher, auf dem Programme und Daten gespeichert werden können. Serienproduktion seit 2010.
- CmCard/SD, CmCard/uSD: Smart Card basierte SD- bzw. Mikro SD-Karte mit Samsung SmartCard Chip aus der Serie S3FS9CI mit zusätzlichem Flash-Massenspeicher, auf dem Programme und Daten gespeichert werden können. Serienproduktion seit 2010.



---

<sup>3</sup> [WIBU03] Security-Evaluation Documents für die in den WIBU-SYSTEMS Hardwaretokens verwendete Sicherheitscontroller: S3FS9CI:  
[http://www.commoncriteriaportal.org/files/epfiles/cible-dcssi2008\\_17en.pdf](http://www.commoncriteriaportal.org/files/epfiles/cible-dcssi2008_17en.pdf) und AT90SC7272:  
[http://www.commoncriteriaportal.org/files/epfiles/cible2005\\_05.pdf](http://www.commoncriteriaportal.org/files/epfiles/cible2005_05.pdf).

*Abbildung 2: Aktuelle CodeMeter Hardware-Token*

Im Unterschied zu normalen Token, die X509-Zertifikate speichern können, um damit eine elektronische Signaturfunktion zu übernehmen, bieten die CodeMeter-Token ein ausgefeiltes Digitales Rechtemanagement-System, das auch unabhängig digitale Rechte vieler unabhängiger Beteiligter speichern kann. Die zugrundeliegenden Verfahren sind international in Europa, USA, Japan und China durch mehrere Patente geschützt, weitere Patentanmeldungen laufen. Im Rahmen von SumoDacs wird die Software und Middleware so erweitert, dass CodeMeter zusätzlich zu den bisherigen Funktionen die eines Standard-Tokens übernehmen kann und den Schutz der Anwenderdaten durch Verschlüsselung in der Gesamtarchitektur ermöglicht. Der Smart Card Chip in CodeMeter ist physisch vom Flashspeicherteil getrennt und wird völlig autonom betrieben und nur von außen angesteuert. Die grundsätzliche Tamper Resistance des Chips wird durch die elektrisch gemeinsame Schnittstelle an USB oder der (u)SD-/CF-Card nicht beeinträchtigt.

Durch die softwaretechnische Realisierung der Middleware auf dem mobilen Client und auch der Softwarekomponenten auf dem SumoDacs Backend Server wird die Sicherheit der Hardware und deren Resistenz gegen Angriffe ebenfalls nicht reduziert, da alle sicherheitsrelevanten Funktionen in der Hardware ausgeführt werden. Dies sind beispielsweise die Signaturberechnung und das Speichern der Private Keys oder der symmetrischen Schlüssel und Lizenzparameter. Das Gesamtsystem, bestehend aus SmartCard Chip, Speicher, Middleware und Software ist nicht nach Common Criteria zertifiziert. Es werden jedoch die Anforderungen und Regeln beachtet, so dass eine spätere Zertifizierbarkeit gegeben wäre. Dies würde jedoch vom Aufwand her das SumoDacs-Projekt sprengen.

Im Projekt war insbesondere die Einbindung des nPA als „Fremdtoken“ (3rd Party-Token aus WIBU-Sicht) als alternativer Sicherheitsanker zu den CodeMeter-Security-Modulen vorgesehen. Hier sollte ein kontaktloses, hochsicheres Ausweistoken zum Zwecke von Authentifizierung in das Architekturkonzept der Sicherheitslösung integriert werden. Die technischen Möglichkeiten und die Infrastrukturvoraussetzungen zur Integration des nPA waren allerdings zu Beginn des Projektes noch nicht in allen Details bekannt.

### **3 PLANUNG UND ABLAUF DES VORHABENS**

Die Laufzeit des Projektes erstreckte sich über 24 Monate (1.11.2009 bis 31.10.2011). Das Projekt gliederte sich in folgende Arbeitspakete wie in Tabelle 1 dargestellt:

Arbeitspakete
AP 1 Vorhabenmanagement
AP 2 Anforderungsanalyse
AP 3 Bedrohungsanalyse
AP 4 Entwurf Gesamtarchitektur
AP 5 Kryptographische Protokolle

## Arbeitspakete

AP 6 Datenmodell für Zugriffskontrolle

AP 7 F&amp;E Backend-Integration

AP 8 F&amp;E Integration Hardware-Token

AP 9 Implementierung mobile Clients

AP 10 Vorgehensmodell

AP 11 Wissenschaftliche Evaluation

*Tabelle 1: Übersicht Arbeitspakete*

Die Verantwortlichkeiten zu den einzelnen Arbeitspaketen verteilen sich gemäß den Kompetenzen der Projektpartner, mit WIBU-SYSTEMS, als koordinierendem Partner, für die Arbeitspakete AP1, AP2, AP4, AP8 und dem Forschungspartner KIT (EISS, AIFB) für AP1, AP3, AP10 und AP11. CAS Software war für die AP7 und AP9 verantwortlich. Darüber hinaus arbeiteten alle Projektpartner an den jeweils anderen Arbeitspaketen aktiv mit. Im Folgenden sollen die einzelnen Arbeitspakete anhand der Merkmale Ziel, Inhalt und Ergebnisse näher erläutert werden:

AP 1	Vorhabenmanagement		
<b>Koordinierender Partner:</b> WIBU		<b>Start:</b> 0	<b>Ende:</b> 24
			<b>Aufwand:</b> 13
<b>Ziel:</b>	Gewährleistung einer effektiven und erfolgreichen Abwicklung des Projekts, Bewältigung von Konflikten		
<b>Inhalt:</b>	1. Vertragswesen, Projektkontrolle 2. Kontinuierliche Vorhabensleitung 3. Konflikt- und Risikomanagement 4. Ergebnisverbreitung		
<b>Ergebnisse:</b>	Kooperationsvertrag, Organisation der Zusammenarbeit, Vertrag über Verwertungsrechte, Projektberichte, Veröffentlichungen, Vorträge, Abschlussbericht		

AP 2	Anforderungsanalyse		
<b>Koordinierender Partner:</b> WIBU		<b>Start:</b> 0	<b>Ende:</b> 3

AP 2	Anforderungsanalyse	
		<b>Aufwand:</b> 16
<b>Ziel:</b>	Bestimmung der Anforderungen, Analyse wissenschaftliches und kommerzielles Umfeld	
<b>Inhalt:</b>	<ol style="list-style-type: none"> <li>1. Anforderungen Endnutzer allg.</li> <li>2. Anforderung Integration</li> <li>3. Anforderung ausgewählte Endnutzergruppe</li> <li>4. Recherche verwandte Arbeiten wissenschaftlicher Bereich</li> <li>5. Recherche verwandte Arbeiten kommerzieller Bereich</li> </ol>	
<b>Ergebnisse:</b>	Dokument Anforderungsanalyse	

<b>AP 3</b>	<b>Bedrohungsanalyse</b>		
<b>Koordinierender Partner:</b> EISS		<b>Start:</b> 1 / 17	<b>Ende:</b> 6 / 21
			<b>Aufwand:</b> 11
<b>Ziel:</b>	Erstellen eines Bedrohungsmodells für die Sicherheitsanalyse		
<b>Inhalt:</b>	1. Identifikation von Angriffszielen 2. Klassifikation von Angriffstypen (etwa extern/intern) 3. Identifikation von realistischen Sicherheitsannahmen 4. Erstellen eines Angriffsbaumes (vorher/nachher)		
<b>Ergebnisse:</b>	Bedrohungsanalyse		

AP 4	Entwurf der Gesamtarchitektur		
Koordinierender Partner: WIBU		Start: 3	Ende: 7
			Aufwand: 21
Ziel:	Entwicklung einer neuen Client-Server Sicherheitsarchitektur		

AP 4	Entwurf der Gesamtarchitektur
<b>Inhalt:</b>	<ol style="list-style-type: none"> <li>1. Architektur mit browserbasierten Zugriff auf Daten und Services eines oder mehrerer Backend-Server unter Einbezug eines zwischengeschalteten DMZ-Servers</li> <li>2. Architektur für zwei mobile Clients</li> <li>3. Analyse aktueller Standards</li> </ol>
<b>Ergebnisse:</b>	<ol style="list-style-type: none"> <li>1. Gesamtarchitektur</li> <li>2. Detailarchitektur für einzelne Komponenten</li> </ol>

AP 5		Kryptografische Protokolle	
Koordinierender Partner: EISS		Start: 3	Ende: 12
			Aufwand: 9
Ziel:	Auswahl und Anpassung geeigneter kryptografischer Verfahren als technische Grundlage für die erreichbare Gesamtsicherheit		
Inhalt:	<ol style="list-style-type: none"><li>1. Identifikation der notwendigen Protokolle für die Netzwerksicherheit</li><li>2. Anpassung der Protokolle an die Verwendung eines sicheren Hardware-Token.</li><li>3. Entwicklung eines Verfahrens für die verschlüsselte Speicherung, das die Schwere von internen Angriffen (etwa durch Viren) beschränkt (Kompartementalisierung).</li><li>4. Untersuchung der Gesamtsicherheit der zusammengesetzten Anwendung (Kompositionalitätsproblem)</li></ol>		
Ergebnisse:	Bereitstellung kryptographischer Verfahren für das Gesamtsystem. Ein Dokument, das die Auswahl und die vorgenommenen Anpassungen nachvollziehbar macht.		

AP 6	Datenmodell für Zugriffskontrolle		
Koordinierender Partner: AIFB		Start: 4	Ende: 16
			Aufwand: 15
Ziel:	Eine Innovation des Projektes liegt in den komplexen Rollenmodellen, die die Person, seine derzeitige Aufgabe und das verwendete Endgerät berücksichtigen. Ziel ist die Entwicklung eines Datenmodells, das diese Aspekte abbildet.		

AP 6	Datenmodell für Zugriffskontrolle
<b>Inhalt:</b>	<ol style="list-style-type: none"> <li>1. Identifizierung relevanter Kontextparameter</li> <li>2. Weiterentwicklung existierender Access Control Modelle für die spezielle Situation mobiler Endgeräte</li> <li>3. Erstellen von Rollenmodellen, die auch die Sicherheit des Endgeräts berücksichtigen</li> <li>4. Sicherung gegen unerlaubten Zugriff durch Verwendung des Hardware-Token</li> <li>5. Benutzerfreundliche Rollenerkennung/Rollenwechsel</li> </ol>
<b>Ergebnisse:</b>	Zugriffskontrollmodell für die Zugriffskontrolle

AP 7	Backend-Integration		
<b>Koordinierender Partner:</b> CAS		<b>Start:</b> 7	<b>Ende:</b> 14
			<b>Aufwand:</b> 21
<b>Ziel:</b>	Funktionale Integration und Datenintegration		
<b>Inhalt:</b>	<ol style="list-style-type: none"> <li>1. Kapselung der Funktionalitäten von Legacy Systemen (Aufwand 8 PM)</li> <li>2. Beispielhafte Umsetzung einer Connection Architecture (Aufwand 5 PM)</li> <li>3. Security-Integration (Aufwand 8 PM)</li> </ol>		
<b>Ergebnisse:</b>	Backend Security Server, Wrapper für verschiedene Legacy-Systeme, offene Schnittstellen und Dokumentation für externe Verwertung		

AP 8	Integration Hardware-Token		
<b>Koordinierender Partner:</b> WIBU		<b>Start:</b> 3	<b>Ende:</b> 20
			<b>Aufwand:</b> 26
<b>Ziel:</b>	Entwicklung der erweiterten Hardware / Runtime mit Browser/Proxy-Server-Unterstützung für offene mobile Endgeräte		
<b>Inhalt:</b>	<ol style="list-style-type: none"> <li>1. Erweiterungen der Firmware (Aufwand 7 PM)</li> <li>2. Erweiterte Runtime / Integration ePA-API (Aufwand 8 PM)</li> <li>3. Integration Browser / Secure Proxy-Server (Aufwand 7 PM)</li> <li>4. Verbesserung der Implementierung des File I/O-Protokolls (Aufwand 4 PM)</li> </ol>		
<b>Ergebnisse:</b>	Hardware-Token in mobile Endgeräte integrierbar, dazu benötigte Software		

AP 9		Implementierung mobile Clients	
<b>Koordinierender Partner:</b> CAS		<b>Start:</b> 6	<b>Ende:</b> 20
			<b>Aufwand:</b> 27
<b>Ziel:</b>	Implementierung von Software-Komponenten für mobile Endgeräte, die ein Push der Sicherheitskomponenten (inkl. Rollen) und erweiterte Netzwerk- und Datensicherheit, Device Management, Profil-Administration etc. erlauben.		
<b>Inhalt:</b>	1. Referenzvorgehen und Dokumentation (Aufwand 8 PM) 2. Implementierung Client für Ultra Mobile PC und spezifischem OS (Aufw. 10 PM) 3. Implementierung Client Mobiles Smart Device und spezifischem OS (Aufw. 9 PM)		
<b>Ergebnisse:</b>	Prototyp UMPC, Prototyp MSD, Best Practice Beschreibung		

AP 10		Vorgehensmodell	
<b>Koordinierender Partner:</b> AIFB		<b>Start:</b> 14	<b>Ende:</b> 22
			<b>Aufwand:</b> 13
<b>Ziel:</b>	Entwicklung eines Vorgehensmodells, wie KMU unter Verwendung von SumoDacs einen sicheren mobilen Datenzugriff realisieren können		
<b>Inhalt:</b>	1. Teilvorgehensmodell Integration DMZ 2. Teilvorgehensmodell Backend-Integration Webapplikation 3. Teilvorgehensmodell Backend-Integration datenbankzentrische Applikation 4. Teilvorgehensmodell Backend-Integration dokumentenzentrische Applikation 5. Teilvorgehensmodell mobile Clients		
<b>Ergebnisse:</b>	Vorgehensmodell		

AP 11		Wissenschaftliche Evaluation	
<b>Koordinierender Partner:</b> AIFB		<b>Start:</b> 20	<b>Ende:</b> 24
			<b>Aufwand:</b> 11

AP 11	Wissenschaftliche Evaluation
<b>Ziel:</b>	Evaluation ausgewählter Projektergebnisse aus Sicht der Nutzer
<b>Inhalt:</b>	1. Evaluation der wahrgenommenen Sicherheit durch Nutzer in speziellen Szenarien 2. Evaluation der Usability der Endnutzerkomponenten 3. Evaluation der Bedrohung und Sicherheit (vorher/nachher)
<b>Ergebnisse:</b>	Evaluationsbericht

Tabelle 2: Übersicht über die Arbeitspakete

Gemäß dem zeitlichen Verlauf und den Zielen aus den Arbeitspaketen wie oben dargestellt wurden die Meilensteine des Projektes so gewählt, dass zu den jeweiligen Zeitpunkten eine nötige Anpassung der Projektplanung und des weiteren Projektablaufes auf Basis der bis dahin gewonnenen Ergebnisse und Erkenntnisse erfolgen konnte. Für einen Projektabbruch wurden Kriterien vorgegeben, wenn die Sinnhaftigkeit des Projektes nicht, oder durch äußere Einflüsse nicht mehr, nicht mehr gegeben sein sollte.

Zeitpunkt	Erreichter Meilenstein und evtl. Auswirkung
<b>M1</b> nach 7 Monaten	Die Sicherheitsanalyse ist abgeschlossen und die Gesamtarchitektur liegt vor.  Abbruchkriterium: Sollte kein Sicherheitsgewinn möglich sein, wird das Projekt abgebrochen.  Steuerungsmöglichkeit: Die vorliegende Sicherheitsanalyse und die Gesamtarchitektur ermöglichen es, den weiteren Projektablauf ggfs. anzupassen.
<b>M2</b> nach 14 Monaten	Ein erster Demonstrator für Backend-Integration und einen mobilen Client liegt vor.  Abbruchkriterium: Sollte sich die Architektur technisch nicht umsetzen lassen, wird das Projekt abgebrochen.  Steuerungsmöglichkeit: Wenn die Umsetzung des Konzeptes auf unerwartete Schwierigkeiten stößt, welche zusätzliche Arbeiten benötigen kann das Arbeitsprogramm angepasst werden. Dazu muss dann evtl. auf die Implementierung eines zweiten mobilen Clients verzichtet werden.
<b>M3</b> nach 20 Monaten	Die Demonstratorentwicklung ist abgeschlossen.  Darauf aufbauend kann die abschließende Evaluation durchgeführt werden.  Steuerungsmöglichkeit: Anpassung des Arbeitsprogramms für die Restlaufzeit

Tabelle 3: Meilensteine



Die Meilensteine wurden ausgenommen von zeitlichen Anpassungen alle erreicht.

#### **4 WISSENSCHAFTLICHER UND TECHNISCHER STAND**

Dieser Abschnitt fasst das technisch-wissenschaftliches Umfeld des Projektes zum Startzeitpunkt kurz zusammen. Dabei wird auf die Konkurrenzsituation und der damalige Stand von Wissenschaft und Technik eingegangen.

Seit dem Zeitpunkt der Antragstellung haben sich eine Reihe wichtiger technologischer Neuerungen vor allem im Bereich der mobilen Geräteentwicklung ergeben. Auch das Thema NFC, Near Field Communication, wurde zum Zeitpunkt der Antragstellung als neues Technologiefeld vorwiegend durch den nPA repräsentiert.

Die Sicherheit für mobile Endgeräte geht oft über Standardtechniken nicht hinaus. Ungelöst ist z.B. das Problem, das sich ergibt, wenn ein Angreifer ein Smartphone durch ein gleich aussehendes Exemplar ersetzt. Der Eigentümer merkt wahrscheinlich zunächst keinen Unterschied und gibt seine Zugangsdaten ein, um das Endgerät bzw. die Anwendungssoftware zu entsperren. Dann kann das manipulierte Endgerät diese geheimen Daten an den Angreifer übermitteln. Nun kann sich dieser wie ein legitimer Benutzer einloggen und das System ohne weitere Einschränkungen benutzen. Für den sicheren Umgang mit mobilen Endgeräten fehlen also sinnvolle 2-Faktor-Authentifikationsmechanismen. Hier könnte die Popularität des neuen Personalausweises dazu beitragen, eine NFC-Schnittstelle in mobile Endgeräte zu integrieren. Somit kann eine zusätzliche Authentifizierung mit dem nPA erfolgen, was die Sicherheit verbessert.

Die Märkte für Mobile Computing und Cloud Computing entwickeln sich sehr dynamisch. Dabei stehen Anforderungen wie Zuverlässigkeit, Bedienbarkeit und geringe Kosten oft vor der Sicherheit. Im Bereich des Mobile Computing ist eine erhöhte Sicherheit oft nur dann möglich, wenn dadurch für den Benutzer nur ein geringer Mehraufwand verbunden ist. Die wirkungsvollsten Sicherheitsverbesserungen der letzten Jahre sind neben Sandboxing vor allem App-Blacklisting (auch Virenschanner genannt). Cloud Computing hingegen lässt sich Sicherheitstechnisch vor allem durch verbesserte Hypervisor und Festplattenverschlüsselung verbessern. Allerdings gibt es keinen wirksamen Schutz gegen Insider-Angriffe und die Sicherheitsmaßnahmen müssen kontinuierlich verbessert werden um im Wettlauf gegen die Hacker den Benutzern eine ordentliche Sicherheit garantieren zu können. Da sowohl auf mobilen Endgeräten als auch in der Cloud sensible Daten gespeichert werden, genügt der Einsatz von Standardmethoden nicht. Durch den Einsatz sicherer Hardware-Token lässt sich die Sicherheit verbessern.

##### **4.1 TECHNISCHER STAND UND KONKURRENZPRODUKTE**

Unter dem Schlagwort „Mobile Security“ finden sich zunächst viele Software-Produkte, die Schutz vor Schadprogrammen wie Viren, Trojanern oder Spyware versprechen. Als Beispiele gibt es hier Produkte von Anbietern wie BitDefender, F-Secure, Symantec, Trend Micro oder Sophos.

Einige weitergehende Sicherheitslösungen für mobile Endgeräte bieten darüber hinaus Features wie VPN-Verschlüsselung, lokale Verschlüsselung, lokale Firewalls von Daten oder eine „Wipeout“-Funktion, um im Falle des Verlusts eines Endgeräts Daten zu löschen. Teilweise sind solche Funktionen auch in „Mobile Device Management“-Lösungen integriert, wobei zusätzlich noch Regeln festgelegt werden können, welche Funktionen auf einem mobilem Endgerät genutzt werden

dürfen, z.B. Installation von Software oder Verwendung des Web-Browsers. Beispiele für solche Produkte sind etwa ubitexx ubi-secure, Sybase Afaria oder der Microsoft Mobile Device Manager. Diese Produkte adressieren jedoch andere Aspekte der mobile Endgeräteintegration mit Backend-Anwendungen und weniger die Sicherheitsprobleme und die Integration von Sicherheitskomponenten, die bei SumoDacs im Vordergrund stehen. Im Projekt geht es vor allem um eine Lösung, die die Anbindung von Browsern an den Token auf der Client Seite und die Einbindung von Backend Servern mithilfe einer DMZ vorsieht.

Desweiteren gibt es spezielle Software-Integrations-Frameworks, um herkömmliche „stationäre“ Unternehmenssoftware auch mit mobilen Endgeräten ansprechen zu können. Als Produktbeispiele sind hier Sybase Onebridge oder Mobileframe zu nennen. Solche Produkte sind jedoch kaum für KMU geeignet und nicht primär auf Sicherheit unter Verwendung eines Hardware-Tokens ausgelegt; „Sicherheit“ ist vielmehr ein Feature unter vielen.

Es gibt auch sog. Identitätsmanagementsysteme, mit denen Unternehmen die eine heterogene IT-Landschaft betreiben, ein einheitliches Identitäts- und Rechtemanagement erreichen können, so dass z.B. ein Arbeitnehmer nicht verschiedene Nutzerkonten samt zugehörigen Passwörtern benötigt. Beispiele für solche Produkte sind etwa: SAP NetWeaver Identity Management, Select Identity / Select Access von HP, Tivoli Identity Manager von IBM, DirX Identity von Siemens. Diese Produkte sind jedoch nicht speziell für mobile Anwendungen oder hardwarebasierte Authentifizierung ausgelegt und für den Einsatz in KMU zu komplex.

Bezüglich Hardware-basierten Security-Token für mobile Anwendungen herrschte zum Zeitpunkt der Antragstellung folgende Markt- bzw. Konkurrenzsituation:

Bisher gibt es  $\mu$ SD-Produkte von den Firmen Certgate, Secusmart und Giesecke & Devrient mit Beschränkung auf die Anwendung der Webauthentifizierung, die aber nur auf speziellen Smartphones mit Krypto-APIs mit spezifischen Treibern lauffähig sind. Die Integration der Security-Token basiert auf SD Card Interface Standards 2.0. Im Projekt SumoDacs war die Unterstützung des nächsten folgenden Standards Release vorgesehen, wurde jedoch sowohl aus hardwaretechnischen als auch aus marktpolitischen Gründen nicht realisiert.

Es gibt noch einige weitere Sicherheitsprodukte für mobile Datensicherheit, die ein Hardware-Token verwenden, z.B. folgende Hersteller wie Gemalto, GeNUCard, SafeNet, Marx, Cryptocard, MXI Security und Discretix für Embedded Systems bieten Hardware-Security-Lösungen. Die meisten dieser Produkte sind jedoch nur für eine beschränkte Anzahl von Plattformen für verfügbar und nicht so vielseitig einsetzbar wie das zu entwickelnde SumoDacs-Token.

Allerdings fehlt den oben genannten Lösungen ein vielseitiges Berechtigungskonzept, wie es mit dem CodeMeter-DRM-System gegeben ist. Mit diesem System ist es möglich, dem dynamisch Rechte für unterschiedliche Rechteinhaber und Sicherheitszonen zu generieren.

Es gibt eine Vielzahl von meist hardwarebasierten Security-Lösungen für Authentifizierung mit Hardware-Token und ggf. zusätzlichen Sicherheitsmerkmalen wie Zugangsschutz zu Secure Storage. Die genannten Hersteller spiegeln nur einen Auszug wieder, von den Firmen die in diesem Umfeld der sicheren Authentifizierung miteinander im Wettbewerb stehen. Eine weitere Besonderheit ist die Anwendung der Features Hardware-Token, Kopierschutz, DRM, sicheres Flash-Memory in

Kombination in einem einzigen Hardware-Token zu vereinen, welches ein hohes Maß an Flexibilität und Mobilität für den Anwender bietet. Die DRM-Lösung erlaubt insbesondere die dezentrale und spontane Förderung von unterschiedlichen Security-Ankern im Token, um damit unterschiedliche Security-Anwendungen parallel betreiben zu können, ohne dass es dazu einer zentralen, die Sicherheit organisierenden Instanz bedürfte.

WIBU-SYSTEMS arbeitet aktiv in der SD Card Association an der Standardisierung des erweiterten Security Interfaces mit und bringt eigene Beiträge im Kontext der Spezifikationen ein. Die eigenen Aktivitäten stehen zum Teil auch im Wettbewerb zu den Standardisierungsbemühungen anderer, international tätiger SDA-Mitgliedsfirmen.

Ansätze, die SIM-Karte für Mobilfunknetze als generelles Hardware-Token zu verwenden, waren zum Zeitpunkt der Antragstellung noch kaum erkennbar. Die SIM-Karte „gehört“ dem jeweiligen Mobilfunkbetreiber und dem einzelnen Kunden bzw. dem einzelnen Kunden, so dass KMUs nicht die Möglichkeit haben, darauf Anwendungen zu implementieren. Allerdings beginnt sich diese Haltung bei den Netzbetreiber grundlegend zu ändern. Offensichtlich wird ein SIM-Sharing mit namhaften Dienstleistern aus dem Finanzbereich als eine Option für weitere Geschäftsanwendungen angesehen.

## **5 ZUSAMMENARBEIT MIT ANDEREN STELLEN**

Das Projekt wurde insbesondere im wissenschaftlichen Bereich genutzt, um mit anderen Stellen im Forschungsbereich Sicherheit und Datenmodellierung zusammenzuarbeiten. Hier sind verschiedene wissenschaftliche Institutionen zu nennen, mit dem ein engerer Wissensaustausch stattgefunden hat.

Im Bereich des nPA wurde mit Anbietern von eID-Services zusammengearbeitet. Dies waren die Firmen Bremen Online Services und ePA-Connect. Sie leisteten im Laufe des Projektes Unterstützung bei der Realisierung der Dienste-Anbindung zum Backend-System zwecks Bereitstellens von nPA-Identitätsmerkmalen ihre Unterstützung in der Entwicklung des Testbetriebes. Ferner wurden verschiedene, zertifizierte nPA-Leser zum Lesen von Testausweisen zur Verfügung gestellt von zwei verschiedenen Herstellern dankenswerterweise zur Verfügung gestellt.

Außerdem wurden Kontakte zu Projekten geknüpft, die sich mit verwandten Gebieten beschäftigen. Dazu gehörte das VOGUE-Projekt. Es konzentriert sich auf die Entwicklung einer integrierten Sicherheitsplattform, so dass mobile Endgeräte vertrauenswürdig auf verschiedenste IT-Systeme (z.B. Lieferketten-übergreifende Applikationen, Unternehmensnetze) zugreifen können.

## **II. SCHLUSSBERICHT (II), EINGEHENDE DARSTELLUNG**

### **1 ERZIELTE ERGEBNISSE**

Die gesetzten Ziele des Vorhabens konnten in den wesentlichen Punkten voll erreicht werden. Stichwortartig sind im Folgenden die Hauptergebnisse aufgelistet, welche in der weiteren Darstellung der Schwerpunktthemen der Projektpartner näher erläutert werden.

Die förderpolitischen und projektspezifischen Ziele wurden erreicht (Übersicht):

#### **Aus wissenschaftlicher Sicht des F&E-Forschungspartners KIT (AIFB, EISS):**

- Schaffung einer gemeinsamen Wissensbasis durch Erstellen der Anforderungs- und Bedrohungsanalyse anwendbar mit Zuschnitt auf die Bedürfnisse von KMUs
- Schaffung einer gemeinsamen Wissensbasis durch Erstellen der Anforderungs- und Bedrohungsanalyse anwendbar mit Zuschnitt auf die Bedürfnisse von KMUs
- Es konnte ein konkreter Zwei-Faktor-Authentifizierungsmechanismus konzipiert und praktisch umgesetzt werden. Die Sicherheit bei Gerätediebstahl und dem sogenannten Shoulder Surfing ist damit maßgeblich erhöht worden.
- Der neue Personalausweis wurde abstrakt modelliert und konnte auf Grundlage dieser Modellierung in die Anwendung integriert werden.
- Es wurde eine abschließende Sicherheitsanalyse unter spezieller Berücksichtigung des Kompositionalitätsproblems erstellt.
- Zur Ermöglichung eines sicheren Offlinezugriffs auf Unternehmensdaten wurde ein Konzept für eine sichere Datenablage erstellt.

#### **Aus Sicht der Industriellen Projektpartner**

Folgende vorbereitende Analysen und Entwicklungsarbeiten an Systemkomponenten wurden durchgeführt:

- Evaluation von Standards und Erstellen einer Anforderungsanalyse
- Identifikation der Anforderungen an das Gesamtsystem und Entwurf einer Gesamtarchitektur
- Integration der CM-Token in das SumoDacs Dreizonenmodell, in die Clients, die DMZ und in das SumoDacs-Backend-System CRM (PIA)
  - Authentifizierung, Autorisierung & Verschlüsselung mit Browserunterstützung
    - Clienseitiger Secure Http-Proxy-Server für webbasierte Authentifizierung
    - Serverseitige Bereitstellung einer Authentifizierungskomponente (Cm-Identity)
    - Bereitstellen lokaler Verschlüsselungs-/Entschlüsselungsfunktionen für die Clientseite, Schutzfunktionen für den Cache-Speicher

- Integration unterschiedlicher Token (CodeMeter USB-Sticks und Flashkarten) für Desktop und mobile Anwendungen auf Zielplattformen
- Einbindung des nPA als Zugangstoken für CodeMeter/CodeMeterAct sowie Integration der License Central in den CodeMeter Authentifizierungsserver -> nPA integraler Bestandteil der SumoDacs Gesamtlösung,
- Bereitstellen und Integration der Authentifizierungskomponenten im Backend-System (Cm-Identity), Anschlussfähigkeit für das Zusammenwirken von Authentifizieren mit kontextsensitiver Zugriffssteuerung
- Vorbereitung der SOpen Source Kompatibilität mit Unterstützung für OpenID-Kommunikationsprotokolle, Bereitstellen von APIs Client- und Serverseitig zur Anbindung von Token mit den Kommunikationsprotokollen
- Integration von CAS Open als Sicherheitsserver in das SumoDacs Drei-Zonen Modell
- Konzeption und Erstellung einer Infrastruktur zu Einbindung von Hardwaretoken (WIBU Codemeter, nPA) in die Authentifizierungsmechanismen von CAS Open, CAS PIA und CAS Mobile Access
- Schaffung eines Frameworks für signaturbasierte Nutzerauthentifizierung für CAS Open, CAS PIA und CAS Mobile Access
  - Schwerpunkt: Entwicklung und Umsetzung des Konzepts „vertrauenswürdiger Clients“ für den Sonderfall des mittelbaren Zugriffs auf den Open Server
- Entwicklung und Integration eines Zwei-Faktor Authentifizierungsverfahrens für CAS Open, CAS PIA und CAS Mobile Access, welches neben Wissen den Besitz eines Hardwaretokens erfordert
- Schaffung eines Frameworks zur Überprüfung der Integrität von Aufrufnachrichten für CAS Open, CAS PIA und CAS Mobile Access auf Grundlage von Hardwaretoken (WIBU Codemeter)
- Einbindung föderierter Authentifizierungsverfahren in CAS Open und CAS PIA auf Grundlage des OpenID Standards  
Konzeption kontextsensitiver Autorisierungsmechanismen für den Zugriff auf Daten und Dienste im Unternehmens-Backend

Die browserbasierte CRM-Software der CAS als SaaS-Lösung verknüpft bislang separate Daten in einem zentralen System und verbindet somit den CRM- und Groupware-Gedanken gekonnt miteinander. Sie verbessert so den Informationsfluss im Unternehmen, beschleunigt die interne und externe Kommunikation und erhöht die Transparenz komplexer Zusammenhänge. Dadurch steigt die Qualität der Informationen über alle Zielgruppen, Kundenbeziehungen werden intensiviert und der Nutzer erzielt aus dieser Informationsverknüpfung große Wettbewerbsvorteile. Sie ermöglicht es, die kompletten Geschäftsprozesse eines Unternehmens, unabhängig von dessen Branche, Größe oder Struktur, einfach und bequem über den Browser in einem einzigen System zu verwalten. Das individuelle oder gruppenbezogene Management von Informationen erfolgt dabei in Echtzeit und vollkommen unabhängig von Ort und Zeit. Durch seinen flexiblen, modularen Aufbau bietet das System eine Unternehmenssoftware nach Maß erhältlich als Software as a Service (Mietvariante). Über den mobilen Zugriff kann man problemlos eine mobile Datensynchronisation zwischen dem CRM System und jeden mobilen Endgerät herstellen.

## **2 ARBEITSPAKETE**

In den nachfolgenden Abschnitten werden die erzielten Ergebnisse aus den Arbeitspaketen (siehe auch Planung und Ablauf) detaillierter beschrieben und den vorgegebenen Zielen gegenübergestellt. Detaillierte, zahlenmäßige Angaben finden sich in Teil I unter Abschnitt

### **2.1 ANFORDERUNGSANALYSE**

Schwerpunkt dieses Arbeitspaketes bildete die Erstellung der Anforderungsanalyse. Hier wurden alle Anforderungen der Endnutzer und die Anforderungen zur Integration der Security-Hardware untersucht. Im Fokus der Untersuchung stehen dabei die Anwendungsbereiche von KMUs. Es werden alle fachlichen Anforderungen erfasst, die für die Integration der geplanten Sicherheitslösung aus Sicht von KMUs erfüllt sein müssen. Desweiteren wurden die Anforderungen an den SumoDacs-Back-End-Server zu definiert, d.h. insbesondere funktionale und nichtfunktionale Anforderungen aus Betreiber-, Forschungs- und Technologiesicht. Ebenso wurden die Anforderungen der Endnutzer ermittelt und/oder antizipiert. Für einen Erfolg des Ansatzes war es entscheidend, dass auch die Perspektive des zukünftigen Anwenders besonders beachtet wurde.

Im Vordergrund standen aus Sicht des Endnutzers die Einfachheit und Einheitlichkeit der Bedienung sowohl für die Desktop-Anwendung als auch für das mobile Smart Phone. Die Integration der Security-Token wie USB, SD Card und microSD sind aus Anwendersicht ergonomisch kein Problem.

Gleiches gilt auch für den nPA, der zunächst als Zugangstoken in der Anwendung für den Desktop eingebunden werden soll. In der ersten Ausbaustufe soll ein bereits zugelassene nPA-Kontaktlosleser in der Basisvariante aber auch mit separatem Pin-Pad zum Einsatz kommen. Verschiedene zertifizierte Leser mit einer Middleware für den Bürger-Client (AusweisApp, OpenLimit) sind mittlerweile unter Windows XP und Windows 7 verfügbar. Damit soll eine einfache Integration des Lesers und des nPA für die Anwendung der Authentifizierungs- und Registrierungsaufgaben im SumoDacs Backend-Server erfolgen. Dazu stehen eID-Server zur Verfügung, die in Verbindung mit Testzertifikaten zu Testanwendungen mit dem nPA genutzt werden können. Für diese Art der Server-Einbindung sind allerdings auch besondere technische Voraussetzungen auf der Seite des Diensteanbieters zu erfüllen. Im Rahmen des AP 4 wird auf die Architektur der Komponenten, die zur Integration des Dienste-Anbieters mit dem eID-Service erforderlich sind, näher eingegangen.

Funktionale Anforderungen an mobile Endgeräte und generelle Optionen der Hardware-Integration der CodeMeter-Schutzhardware im Hinblick auf marktrelevante Betriebssystemumgebungen wurden auf der Basis von Standards untersucht. Die Funktionalität und die derzeitigen marktgängigen Integrationen von NFC-Lesern für mobile, respektive portable Endgeräte wurden mit Blick auf den Stand derzeitiger Lösungen am Markt sondiert. Hard- und Softwareschnittstellen im Umfeld NFC- und RFID-Lösungen sowie relevante Standards und Tendenzen in den Standardisierungsgremien wurden recherchiert. Recherchen über verwandte Arbeiten im wissenschaftlichen Bereich wurden ebenfalls durchgeführt.

Eine weitere Recherche im kommerziellen Bereich befasste sich allgemein mit der Situation von Trust-Infrastrukturen basierend auf elektronischen Identitätskarten, in Deutschland und in Europa, soweit sie als nationale eID-Cards mit hoheitlichem Charakter im Einsatz sind und im Rahmen von Public Private Partnerships auch in kommerziellen Anwendungen für Authentifizierungs- und

Signaturaufgaben Einsatz finden. Verglichen wurde dies mit der Ausgangssituation von Trust-Infrastrukturen und deren vereinheitlichter Nutzungsmöglichkeit in den USA, wo noch kein nationales Programm für eine Einführung einer einheitlichen eID-Karte im Sinne einer hoheitlichen Citizen-Card besteht. Andere Lösungen auf der Basis von offenen Identity-Standards werden derzeit erprobt und unter einem föderativen System von Trust Frameworks interoperabel gehalten, wobei nach Stufen einer gewährten Vertrauenswürdigkeit (Assurance of Trust) unterschieden werden kann.

## **2.2 BEDROHUNGSANALYSE**

Um die Sicherheit der im Projekt entwickelten Dienste beurteilen zu können, wurden in AP3 diesbezügliche Bedrohungen systematisch ermittelt und analysiert. Hierzu wurden zunächst die folgenden Angriffsobjekte ermittelt:

- das mobile Endgerät (z.B. Diebstahl, Manipulation, Malware)
- der Applikations- und Dokumentenserver (v.a. durch interne Angreifer)
- der Sicherheitsserver, d.h. das SumoDacs-Gateway, (darüber Zugang zu sensiblen Daten, z.B. Denial-of-Service-Angriffe)
- Firewalls (als "Einfallstor" für nachgelagerte Angriffe auf mobile Anwendungen, Sicherheits- und Applikationsserver)

Zur Antizipierung von Angriffsvektoren wurden verschiedene Angriffsziele identifiziert. Zu nennen wären hier das unbefugte Lesen oder Schreiben (d.h. verändern, hinzufügen oder löschen) von Daten, das Unverfügbarmachen von Daten (etwa durch Sabotage), sowie das Vortäuschen von Daten (z.B. durch Vortäuschen der SumoDacs-Infrastruktur).

Weiterhin wurden verschiedene Angriffstypen identifiziert. Angriffstypen dienen dazu die grundsätzliche Methodik von Angriffen zu systematisieren. Hierzu werden die unterschiedlichen möglichen Ausgangssituationen eines Angriffs berücksichtigt, etwa wird zwischen einfachen und privilegierten Benutzern sowie Mitarbeitern der Anbieter und externen Angreifern unterschieden. Zu unterscheiden sind genauer:

- Interne und externe Angreifer (interne Angreifer sind grundsätzlich autorisiert, missbrauchen jedoch ihre Zugangsrechte, externe Angreifer haben keinen Zugang)
- Online- und Offline-Angriffe (betrifft den Interaktionsgrad des Angriffes, Online-Angriffe stellen wegen ihrer Dynamik höhere Anforderungen an Angreifer als offline durchgeführte)
- Social Engineering (aufgrund zwischenmenschlicher Interaktion werden Sicherheitsschwächen geschaffen)

Durch die unterschiedlichen Zugriffsrechte und Angriffsvoraussetzungen, die sich aus den Angriffstypen ergeben, ergeben sich unterschiedliche Bedrohungen für die Sicherheit. Diese erfordern entsprechend angepasste Sicherheitsmaßnahmen. Als Grundlage zu deren Entwicklung wurde eine Liste an realistischen Sicherheitsannahmen aufgestellt.

Für mögliche Bedrohungen relevant ist auch die Vergabe von Zugriffsrechten. Es wurden verschiedene Merkmale identifiziert, auf denen die Vergabe von Zugriffsrechten beruhen sollte:

- Identität des Benutzers (Zugang mit Login-Name und Passwort, zusätzlich z.B. auch der neue Personalausweis mit NFC-Technologie)
- Rolle des Benutzers (z.B. für feingranularen Zugriff)
- Gerätestatus (z.B. Fähigkeiten des Gerätes wie Ende-zu-Ende- oder Speicherverschlüsselung)
- Token (z.B. in USB- oder Speicherkartenform getrennt mitgeführt)
- weitere Merkmale wie IP-Adresse, Aufenthaltsort, Uhrzeit (z.B. Beschränkung von Zugriffsrechten auf einen bestimmten Aufenthaltsort zu einer bestimmten Uhrzeit)

Weiterhin wurde ein systematischer Angriffsbaum erstellt, der aus einem Teilbaum je Angriffsziel besteht. Diese Bäume stellen übersichtlich dar, was ein Angreifer tun müsste, um das entsprechende Angriffsziel zu erreichen.

### **2.3 ENTWURF DER GESAMTARCHITEKTUR**

Der Entwurf der Gesamtarchitektur des SumoDacs 3-Zonen Modells wurde mit Meilenstein 1 fertig gestellt. Dem DMZ-SumoDacs-Server (DMZ-SD-Server) kommt im Rahmen des Gesamtkonzeptes eine zentrale Steuerungsfunktion für User-Authentifizierung zu. das gesteuert bzw. geroutet werden. Der Rechtemanagement-Services sowie das Management kontextsensitive Zugriffe kann nicht auf der DMZ-Seite abwickelt werden, da die Steuermechanismen für den Zugriff auf Anwendung und Daten im Serverprozess des Datenbanksystems ablaufen müssen, da nur dort Plausibilitätsprüfungen aus Gründen der Server-Architektur der Performance zweckmäßigerweise erfolgen können. Erläuterungen zur Integration der DMZ in die Back-End Services ( CRM-Application-Server sowie ERP-Application-Server sowie Dokumenten-Server) sind im Abschnitt Backend-Integration zu finden. Berücksichtigung in der Auslegung der Ende-zu-Ende Security im Backend finden. Aus der Sicht der Gesamtarchitektur sind noch weitere Detail-Fragen zu beantworten. Bei der Anwendung und Adaption von Protokollstandards zur Integration des CodeMeter-DRM-Systems in der DMZ boten sich zwei Alternativen. Eine interoperable OpenID- oder SAML- Standardschnittstelle ergab sich grundsätzlich als Option für eine standardisierte Kommunikation mit dem Backend-System. Eine sich Open-ID orientierende Protokoll-Lösung wurde als erster Schritt für die Integration in eine User-Authentifizierungslösung bevorzugt.



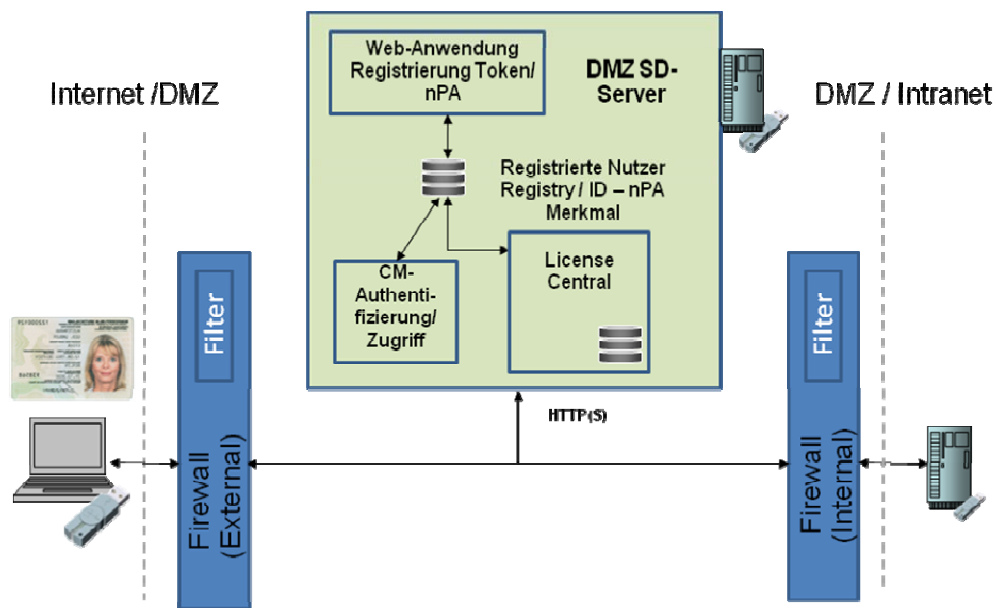


Abbildung 3: Firewalls und SumoDacs Sicherheitsserver, 3-Zonen Modell

Die Integration des nPA als Identity-Token in der Anwendung mit CodeMeter wurde im Konzept für die Gesamtarchitektur festgelegt. Auch die prinzipielle Möglichkeit der Integration des nPA in das softwarebasierte System CodeMeterAct (CmAct) für mobile Betriebssysteme wurde auf der Basis von Lösungsvorschlägen festgelegt.

CmAct kann in unterschiedlichen Methoden mit einem dedizierten Hostsystem über den Weg der Merkmalsbindung logisch verbunden werden. Eine Methode sieht die rein statische Bindung mit den unverwechselbaren Identitätsmerkmalen des Hostrechners vor. In diesem Kontext bietet die Bindungstechnik einen automatisierten und für einen gewünschten Schutzlevel skalierbaren Bindungsprozess, der auf die spezifische Anwendung bezogen flexibel von einem Lizenzgeber implementiert werden kann.

Eine andere Methode, die hier im Entwicklungsvorhaben für den Einsatz mit dem nPA entwickelt und implementiert wurde, bietet die Möglichkeit der Nutzung einer dynamischen hergestellten (sporadischen) Bindung von CmAct an ein standardisiertes Identity-Token wie den nPA. Der nPA bietet seinerseits die Anwendung der eingebetteten elektronischen Identität im nationalen Ausweisdokument unter Bereitstellung höchster Sicherheitsfunktionen. Sie dienen für die Identifikation und Authentifizierung mit allen auch hochvertrauenswürdigen Webanwendungen. Großer Komfort ergibt sich daher in der Anwendung, da seitens der Anwendungsfelder aufgrund der hohen Sicherheit keine Einschränkungen gegeben sind. Die Nutzung des nPA mit dynamischem Bindungsprozess hat gegenüber einer vorzugsweisen statischen Bindung an einen dedizierten Host den Vorteil, dass dem mobilen Nutzer der spontane Zugang zu einer Anwendung, z.B. Webanwendung, offen steht, sofern neben dem zertifizierter Leser eine mindestens zeitweilig zur Verfügung stehende Online-Verbindung vorhanden ist. Der Mechanismus zur Aktivierung und zeitlich begrenzten Nutzung einer CmAct-Lizenz kann wie bei beim Bindungsprozess für statisch implementierte Bindung in einem sehr einfachen und voll automatisierten Ablauf mit der Präsentation des nPA und der Eingabe der PIN angestoßen werden.

Die nachfolgende Darstellung zeigt in einem vereinfachten Funktionsschaubild die Architekturkomponenten, die für die Vernetzung von CodeMeter mit der Infrastruktur des nPA und in der Anbindung an den Backend-Server wesentlich sind.

Die einzelnen Schritte, die im Protokollverlauf aufeinander folgen müssen, damit die Bereitstellung einer zeitweilig aktivierten Lizenz zur Freischaltung einer geschützten Anwendung erfolgt, werden nachfolgend erläutert (siehe auch Abbildung).

**Schritt 1:** Das Starten der Anfrage nach einer Dienste-Anwendung erfolgt im Browser oder aus einer Client-Anwendung.

### Übersicht Architektur nPA / eID-Server / CodeMeter

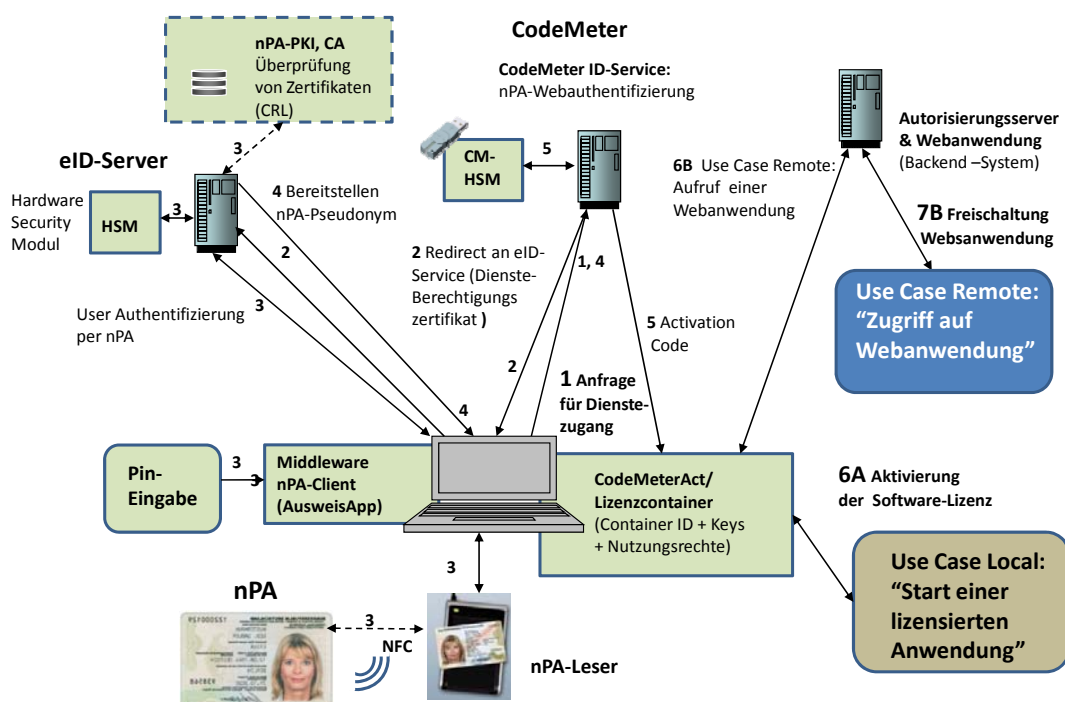


Abbildung 4: Übersicht nPA-Demonstrator

**Schritt 2:** Die Web-Anwendung (hier der CodeMeter ID-Service) der wird über ein Re-direct auf den eID-Server zur Authentifizierung mit den nPA umgeleitet. Die Webanwendung authentifiziert sich mit einem Diensteberechtigungszertifikat, um für den Zugriff autorisierte nPA-Daten übermittelt zu bekommen.

**Schritt 3:** Die Kommunikation zwischen eID-server und der AusweisApp wird eingeleitet, die Komponenten (Leser und AusweisApp) authentifizieren sich, sodass eine sichere Ende- Ende-Verbindung zwischen dem nPA und dem HSM des eID-Servers hergestellt werden kann. Die PIN-Eingabe schaltet die Kommunikation frei, damit anschließend das Auslesen der Identity-Parameter aus dem nPA nach Maßgabe der autorisierten Zugriffsberechtigung erfolgen kann. Der eID-Server

kann ggf. die Gültigkeit des Dienste-Zertifikates mit Hilfe einer Zertifizierungsinstanz auf aktuelle Gültigkeit überprüfen. Anschließend wird das Auslesen der Parameter (hier das im nPA gespeicherte Pseudonym) vom User freigegeben.

**Schritt 4:** Der eID-Server stellt das Merkmal dem CodeMeter eID-Service zur Verfügung. Die Identifikation des Nutzers wird anhand des Registers vorgenommen, in welchem alle zugelassenen Nutzer mit ihren Nutzungsrechten gespeichert sind.

**Schritte 5, 6A und 6B:** Mit Hilfe des CodeMeter-Masterdongle (der „HSM“ für den Anwendungsbereich von CodeMeter) wird der Activation Code generiert und an den Lizenzcontainer im Computer des Nutzers gesendet. Dort steht die dynamisch generierte Lizenz für die zeitlich befristete Nutzung der Anwendung bereit. Diese kann je nach Anwendungsfall die Nutzung einer „entfernten“ Anwendung freischalten, z. B. den Webzugang zu einer Unternehmensanwendung (Schritte 6B und 7) oder die Aktivierung einer CodeMeter geschützten Anwendung wie im „Use Case Local“ ermöglichen (Schritt 6A).

**Schritt 7:** Nach dem Aufruf der gewählten Webanwendung durch den Browser wird der Autorisierungsserver ein Zugangstoken mithilfe des Lizenzcontainers generieren und gemäß der Zugangsberechtigung die gewünschten Funktionen in einer Webanwendung freischalten.

Der Einsatz des nPA erlaubt in Kombination mit CodeMeter/CodeMeterAct die Nutzung einer vorhandenen, hochsicheren Infrastruktur zur Identifikation und Registrierung eines Anwenders zur Nutzung von beliebig vielen Anwendungen. Durch die enge Verzahnung der Hardware Security Komponenten (HSM) in den Back-end Systemen lässt sich auf Protokollebene ein vergleichsweise gut gesichertes Schutzsystem für Rechtemanagement und Zugangskontrolle erzielen. Ein Anwendungsfall für Zugangsmanagement stellt bei Entertainment-Diensten zum Beispiel die vertrauenswürdige Nutzung der Altersverifikation mittels des nPA dar. Unter Anwendung einer durchgängig hardwarebasierten CodeMeter Security-Lösung lassen sich daher sehr sichere Zugangskontrolldienste sowie komfortabel anwendbar DRM-Dienste aufsetzen.

Im Vorhaben wurde von den beiden Lösungsmöglichkeiten der Weg 7 beschritten.

Für die technische Nutzung der Sicherheitstoken beim Client ist eine Einbindung in die Software unumgänglich. Für die Realisierung der clientseitigen Nutzung mit mobileren Geräteformen (Smartphone, Tablet usw.) ist eine getrennte Brücken-Lösung entwickelt worden, der SumoDacs-Client. Diese ist analog einem lokalen Proxy realisiert. x veranschaulicht das Zusammenspiel der verschiedenen Komponenten.

### Architecture of the PIA system with the token

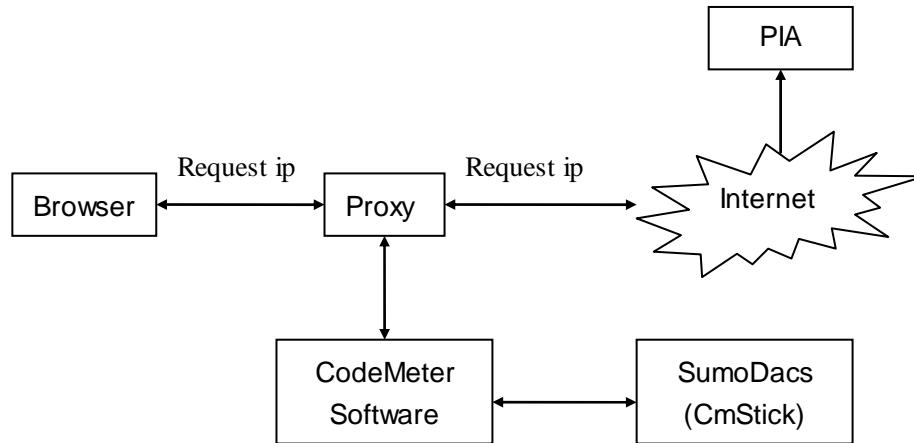


Abbildung 5: Einbindung der Hardware-Token

Anfragen des Browsers („HTTPS-Request“) werden an den SumoDacs-Client übergeben. Dazu wird entweder der SumoDacs-Client als Proxy im Browser festgelegt oder er wird in der URL über einen speziellen Port adressiert. Sind diese Anfragen nicht an eine SaaS-Anwendung über den SumoDacs-Sicherheitsserver gerichtet werden diese wie bei einem Proxy bearbeitet. Bei Anfragen an den SumoDacs-Server wird für diese Anfrage ein Authentifizierungsmerkmal (Challenge) beim SumoDacs-Server über einen Webservice angefragt. Der SumoDacs-Client gibt diese an die CodeMeter®-Runtime weiter. Diese wiederum lässt durch den CmDongle eine entsprechende Antwort (Response) berechnen. Diese wird an die ursprüngliche Anfrage angefügt und kann vom SumoDacs-Server geprüft werden. Ist diese korrekt, wird die Anfrage ausgeführt, andernfalls erhält der Nutzer eine Fehlermeldung. Durch die Verwendung von Private-Public-Kryptographieverfahren wird eine gegenseitige Authentifizierung sichergestellt. Der SumoDacs-Client und die CodeMeter®-Runtime sind auf das jeweilige Betriebssystem anzupassen. Bisher liegen Implementierungen für Windows und WindowsMobile vor. Eine Entwicklung für Android wurde noch nicht angegangen ist aber im Rahmen von Weiterentwicklungen in Arbeit.

Abbildung 6 zeigt die im Rahmen von SumoDacs entwickelte Architektur zur Integration bestehender stationärer Unternehmenssysteme (Legacy-Systeme, Backend-Bereich) und zur Bündelung der von diesen Systemen bereitgestellten offenen Dienste über ein Gateway.

Die Gatewayfunktionalität wird durch einen entsprechend erweiterten CAS Open Server realisiert, der Dienste der angebundenen Legacy-Systeme nach außen über die drei Protokolle REST, SOAP und Java RMI verfügbar macht. Das Gateway übernimmt dabei die zentrale Authentifizierung der Request auf Grundlage der darin übermittelten User Credentials. User Credentials können um Kontextinformationen, beispielsweise den Aufenthaltsort des Nutzers, die Uhrzeit oder die Konnektivität des anfragenden Clients angereichert sein. Der Credential-Typ bestimmt das anzuwendende Authentifizierungsverfahren. Auf seiner Grundlage wählt die Authentication Facade

eine oder, im Falle von Zwei-Faktor-Authentifizierung, mehrere zuständige Authentication Provider aus. In SumoDacs wurde eine Unterstützung für OpenID Credentials und Zwei-Faktor Authentifizierung über mit digitalen Signaturen kombinierte Single-Sign-On Token (SSO) bzw. klassische Passwörter umgesetzt. Die Entkopplung über die Authentication Facade und die als Plug-Ins ausgelegten Authentication Provider garantieren dabei die zukünftige Erweiterbarkeit des Systems um zusätzliche Authentifizierungsverfahren.

Erfolgreich authentifizierte Aufrufe werden durch die Request Routing Schicht des Gateways an den Konnektor des Zielsystems weitergeleitet. Ein Konnektor setzt sich aus einer Autorisierungs- und einer Adapterkomponente zusammen. In der Autorisierungskomponente erfolgt die zielsystemspezifische Autorisierung des Aufrufs, wobei hier die ebenfalls die Auswertung der im Request enthaltenen Kontextinformationen möglich ist. Die Adapterkomponente nach erfolgreicher Autorisierung für den Aufruf des jeweiligen Legacy-Systems und die Übergabe des Ergebnisses an die Request Routing Schicht verantwortlich.

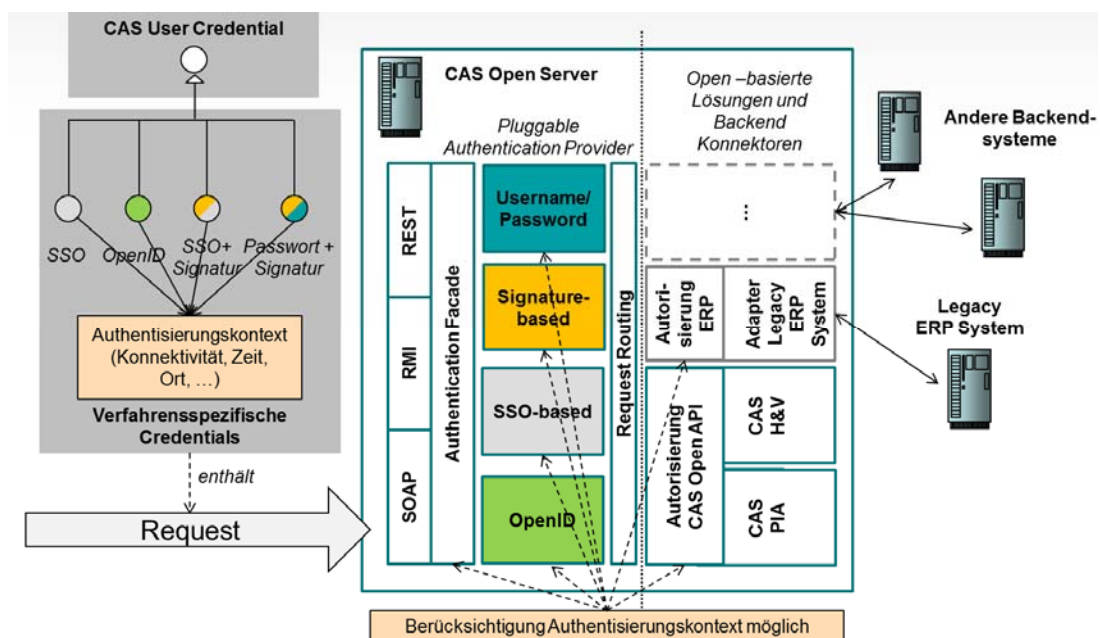


Abbildung 6 Backend-Integration mit cas open

## 2.4 KRYPTOGRAPHISCHE PROTOKOLLE

In AP5 wurden die für die Netzwerksicherheit notwendigen Protokolle identifiziert und an die Verwendung mit einem sicheren Hardware-Token angepasst. Weiterhin wurde ein Verfahren für die verschlüsselte Speicherung entwickelt. Abschließend wurde die Gesamtsicherheit der zusammengesetzten Anwendung analysiert.

Zunächst wurden die beteiligten Parteien (Benutzer, Endgerät, Hardware-Token, neuer Personalausweis und Server) identifiziert und nach ihren Fähigkeiten und Funktionen klassifiziert.

Hierzu wurden der neue Personalausweis sowie das Hardware-Token (nach dem CodeMeter-Token der Firma WIBU-Systems) abstrakt modelliert.

Als wichtiges Entwurfsziel wurde vereinbart, möglichst wenige elementare Protokolle im Gesamtentwurf zu verwenden. In weiten Teilen konnte auf bereits bestehende Technologien zurückgegriffen werden. Zur Absicherung der Kommunikation (Vertraulichkeit und Integrität) etwa wird das etablierte Protokoll Transport Layer Security (TLS) verwendet. Im Gegensatz zum gewöhnlichen Einsatz empfiehlt sich hier jedoch die gegenseitige Authentifizierung von SumoDacs-Server und Endgerät.

Es wurde eine verbesserte Variante des Passmaze-Protokolls beschrieben, mit der sich Benutzer und Smartphone mit Token gegenseitig authentifizieren. Damit werden die starken Angriffe abgefangen, bei denen das Endgerät manipuliert oder durch ein gleich aussehendes Gerät ersetzt wird.

Zum Offline-Zugriff auf die Daten bei fehlender Serververbindung wurde ein performantes Verfahren zur verschlüsselten Speicherung heruntergeladener Daten entwickelt, das keine Anpassung des Betriebssystemkerns erfordert und mit Hilfe des Tokens eine sichere Speicherung auf Applikationsebene realisiert. Bei Verlust des Hardware-Tokens ist es dem vertrauenswürdigen Server möglich, ein neues, äquivalentes Token zu programmieren, mit dessen Hilfe die verschlüsselten Daten auf dem Smartphone gerettet werden können.

Um zu entscheiden, ob sich ein Benutzer einloggen darf und welche Rechte ihm zugestanden werden, wurden verschiedene Kontextparameter untersucht. Diese werden in Arbeitspaket 6 verwendet, um sogenannte Kontextschalter zu realisieren.

Abschließend wurde unter Berücksichtigung des Kompositionalitätsproblems eine Analyse der Gesamtsicherheit durchgeführt. Alle bei der Analyse gefundenen etwaigen Schwachstellen lassen sich durch Standardmechanismen beheben.

Das CodeMeter DRM-System wurde dem Forschungspartner EISS auf der Basis von Software Development Kits (SDK) zur Verfügung gestellt. Die einzelnen SDK-Komponenten wurden vom EISS erprobt und die Rolle der kryptographischen Protokolle untersucht.

Relevante Standards wie SAML 2.0 und XAML sowie OpenID für Identity Management wurden auf Anwendbarkeit im Hinblick auf die geplante Gesamtarchitektur und erforderliche Interoperabilität bei der Anwendung kryptographischer Standards untersucht. Grundsätzlich ergaben sich keine technischen Probleme seitens des CodeMeter-Systems, die geforderten Protokolle aus der Sicht anzuwendender Kryptographie (Bereitstellung durch Hardwarefunktionen) unterstützen zu können. Die Arbeiten im Vergleichs- und Bewertungsprozess zur Herstellung von Interoperabilität mit Authentifizierungsstandards sind soweit abgeschlossen. Dies betrifft auch das Konzept für eine Integration der externen eID-Schnittstelle in eine CodeMeter ID-Webanwendung auf der Basis von SAML.

## **2.5 DATENMODELL FÜR ZUGRIFFSKONTROLLE**

Im Folgenden werden - neben einer allgemeinen und knappen Darstellung von Zugriffskontrollmodellen - die Schritte erläutert, welche notwendig waren, um das Datenmodell für die Zugriffskontrolle zu erstellen. Darauf folgt ein kurzer Überblick über das entwickelte Modell,

welches konkret für das Projekt verwendet wurde. Auch wird auf das Vorgehen bei der Erstellung der Kontextparameter eingegangen.

Zugriffskontrollmodelle (kurz: ZKM) sind die formale Beschreibung von natürlichsprachlichen Sicherheitsanforderungen (sog. Sicherheitspolitiken, Security Policies). Solche Sicherheitsanforderungen können etwa in Form von Gesetzen, Anforderungsdokumenten oder Arbeitsvorgaben vorliegen. Es werden drei Grundformen von ZKM unterschieden: Discretionary Access Control (DAC), Role-based Access Control (RBAC) und Mandatory Access Control (MAC). Letzteres wird hauptsächlich im Hochsicherheits-Bereich (z.B. Militär oder Geheimdienst) eingesetzt oder um „Versteckt im Hintergrund“ zusätzlich zu DAC oder RBAC bestimmte Fehler abzufangen und war für das Projekt nicht von großer Bedeutung.

Die Grundidee von Discretionary Access Control (DAC) ist es, dass der Nutzer, der eine bestimmte Ressource (z.B. Datei, Datenbankobjekt) erzeugt hat, für diese zunächst alle Berechtigungen hat (z.B. Lesen, Schreiben, Löschen, Ändern, Anhängen) und diese nach eigenem Ermessen an andere Nutzer weitergeben kann [Lamp74]<sup>4</sup>. Man nennt DAC deshalb auch „benutzerbestimmbare Zugriffskontrolle“. DAC folgt also dem Eigentümer-Prinzip. Eine Berechtigung kann auch an Gruppen von anderen Nutzern weitergegeben werden. Es kann auch vorgesehen sein, dass der Empfänger einer Berechtigung diese wiederum an andere Nutzer weitergeben kann.

Bei Role-based Access Control (RBAC) können einem Nutzer *ausschließlich* über Rollen Berechtigungen zugewiesen werden [FeKC07]<sup>5</sup>. Rollen werden gemäß Aufgabenbeschreibungen in Unternehmen/Organisationen definiert, z.B. „Vertriebsleiter“, „Vorstandsmitglied“ oder „Praktikant“. Diesen Rollen werden dann die eigentlichen Berechtigungen zugewiesen, z.B. bestimmte Operationen auf bestimmten Daten durchführen zu dürfen. Es ist *nicht* zulässig, einem Nutzer direkt (also ohne den „Umweg“ über eine Rolle) Berechtigungen zuzuweisen wie in DAC. Weiter können RBAC-Modelle noch Vererbungsbeziehungen zwischen Rollen vorsehen sowie die Definition von sich gegenseitig ausschließenden Rollen zur Realisierung von statischer und dynamischer „Separations of Duties“.

Für die Entwicklung des Berechtigungsmodells in SumoDacs wurde zunächst das Grundmodell der Software „CAS PIA“ in Form eines UML-Klassendiagramms aufgezeichnet. Diese Notationsform wurde gewählt, weil sie im Bereich der Software-Entwicklung weit verbreitet ist und für die Beschreibung solcher Modelle eine hinreichende Mächtigkeit hat [Kech05]<sup>6</sup>. Eine grafische Notation ist für die Diskussion des Modells mit mehreren Beteiligten besonders geeignet, z.B. durch Ausdruck auf ein A3-Blatt oder Darstellung mittels Notebook & Beamer.

---

<sup>4</sup> Lamp74: Lampson, B.W.: Protection. Operation Systems Review, vol. 1., no. 8, 1974, Seite 18-24.

<sup>5</sup> FeKC07: Ferraiolo, D.F., Kuhn, D.R., Chandramouli, R.: Role-Based Access Control (2<sup>nd</sup> Edition). Artech House, Boston (USA) and London (U.K.), 2007.

<sup>6</sup> Kech05: Kecher, Christoph: UML 2.0 — Das umfassende Handbuch. Galileo-Computing-Verlag, Bonn, 2005.

Für die Erstellung eines ersten Modells wurde zunächst auf die Endnutzer-Dokumentation zurückgegriffen. Weiter stand ein Testaccount für CAS PIA zur Verfügung. Das auf Grundlage dieser Ressourcen entwickelte Modell berücksichtigte aber zahlreiche Merkmale des tatsächlich implementierten Berechtigungsmodells nicht, da in der aktuellen Version noch nicht der Zugriff auf alle Merkmale umgesetzt ist. Für manche Kundengruppen / Installationen sollen auch nicht alle Merkmale zur Verfügung stehen. Es ist denkbar, dass in zukünftigen Versionen von CAS PIA über eine Erweiterung der Nutzerschnittstelle Zugriff auf weitere Merkmale des Berechtigungsmodells gegeben werden. Es wurde deshalb das so entwickelte Modell mit dem zuständigen Chef-Architekt in mehreren Iterationen diskutiert und entsprechend überarbeitet. Das auf diese Weise erstellte Modell wurde dann im Rahmen eines Projekttreffens allen Projektpartnern vorgestellt. Eine weitere interessante Erfahrung bei der Erstellung des Modells war, dass es nicht immer einfach ist, abzugrenzen, ob eine Komponente noch zum Berechtigungsmodell oder zum „normalen“ Datenmodell gehört.

Für die Wahl möglicher Kontext<sup>7</sup>-Parameter, die für die Zugriffskontrollentscheidung erhoben werden können, wurde u.a. eine entsprechende Recherche in der wissenschaftlichen Literatur durchgeführt. Das genaue Vorgehen wird später im Abschnitt Vorgehensmodell beschrieben.

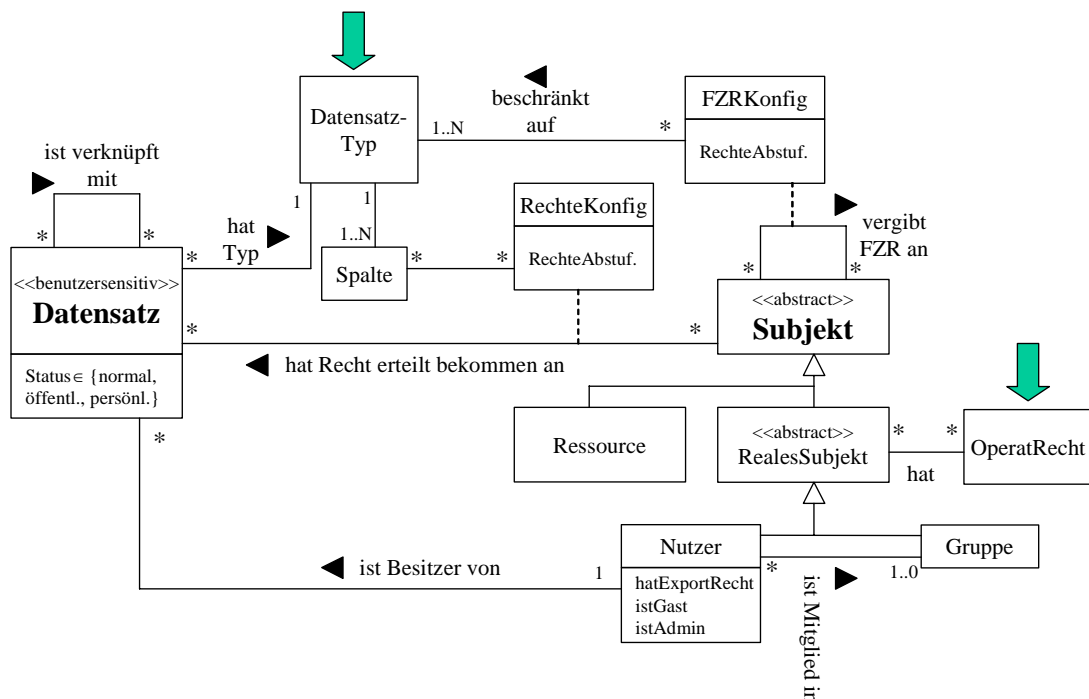
Das entwickelte Zugriffskontrollmodell ist in Abbildung 7 in Form eines UML-Klassendiagramms dargestellt. Da für einzelne Objekte den Nutzern direkt Berechtigungen zugewiesen werden können, ist das Modell als „Discretionary Access Control“ (DAC, benutzerbestimmbare Zugriffskontrolle) einzuordnen.

---

<sup>7</sup> Unter Kontext wird im Rahmen des Projekts jede Form von zur Laufzeit in expliziter Form für das System verfügbare Information verstanden, mit dem eine dynamische Anpassung an die aktuelle Situation des jeweiligen Nutzers vorgenommen werden kann [Dey01].

Dey01: Dey, A.K.: Understanding and Using Context. Personal and Ubiquitous Computing Journal, vol. 5, no. 1, 2001, Seite 3-7.





#### Legende:

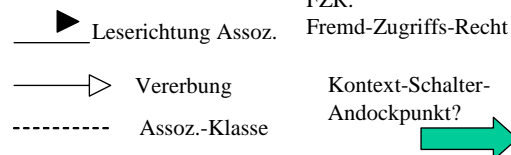


Abbildung 7: Berechtigungsmodell mit Kontext-Schaltern

Welche Kontextschalter im Einzelnen verwendet werden müssen, hängt von der Situation ab, die es abzubilden gilt. Zunächst müssen relevante Situationen beschrieben werden. Anschließend müssen die entsprechenden Situationen mit maschinell bearbeitbaren Parametern eindeutig beschrieben werden. Schließlich muss geprüft werden, ob die technischen Möglichkeiten existieren, um die relevanten Kontextparameter zu erfassen und ob sie mit der (neu-/weiter-)entwickelten Anwendung bzw. dem eventuell schon bestehenden System kompatibel sind. Gegebenenfalls muss eine Situation nochmals durchdacht werden, um eventuell andere Parameter zu finden. Sofern die Anforderungen erfüllt werden können, kann mit der Entwicklung bzw. der Integration von Kontextschaltern begonnen werden.

Abhängig von bestimmten Kontext-Parametern werden dynamisch zur Laufzeit des Systems die sogenannten „Kontextschalter“ ein- und ausgeschaltet. Kontextschalter können Entitäten oder auch Assoziationen sein, mit denen Entitäten einander zugeordnet werden können.

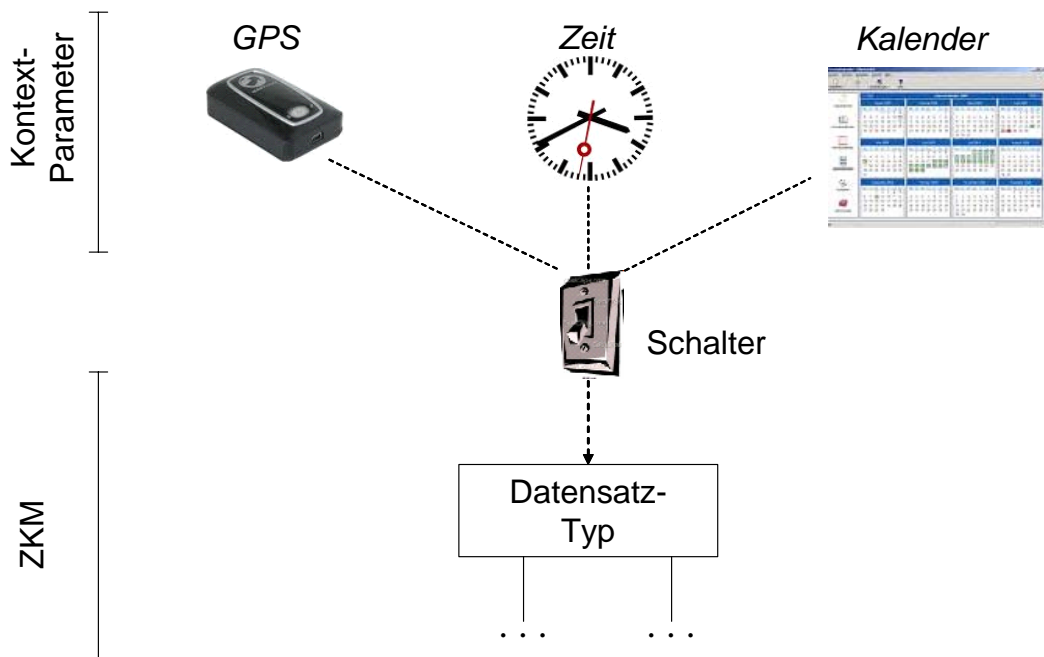


Abbildung 8: Prinzip "Kontext-Schalter"

Im Modell wurden zwei Stellen identifiziert, die besonders dafür geeignet sind, als Andockpunkte für „Kontextschalter“ zu fungieren: Operationale Rechte und Datensatztyp. „Operationale Rechte“ bieten sich als Ziel eines Kontext-Schalters an, da sie u.a. die Berechtigung für den mobilen Zugriff beinhalten. Mit Kontext-Schaltern für bestimmte Datensatztypen kann der Zugriff auf besonders sensitive Objekttypen unter bestimmten Bedingungen untersagt werden. Durch die Möglichkeit, an verschiedenen Komponenten des Berechtigungsmodells Kontext-Schalter anzubringen gewinnt das Modell an Flexibilität.

Weiter wurde noch ermittelt, welche Kontext-Parameter sich für diese Kontext-Schalter eignen: Ortung Endgerät, Art der Authentifizierung, (Orts-)Zeit und Termine. Die Ortung des Endgerätes kann beispielsweise über GPS (Eigenortung des mobilen Computers) oder die Auswertung der verwendeten IP-Adresse (als Fremddortung durch das Backend) vorgenommen werden. Es kann so etwa der mobile Zugriff von im Ausland befindlichen Mitarbeitern auf alle Datensätze vom Typ „Personalakte“ verhindert werden.

Mit „Art der Authentifizierung“ ist gemeint, ob der Nutzer nach dem herkömmlichen Verfahren mit einem Nutzernamen und einem Passwort am System angemeldet hat, oder ob er zusätzlich eine CodeMeter-Smartcard (Token) verwendet hat. Bei der Smartcard-basierten Authentifizierung wird zur Authentifizierung ein auf der Smartcard sicher gekapselter privater Schlüssel verwendet. Hardware-basierte Authentifizierung bietet ein wesentlich höheres Maß an Sicherheit als die Verwendung von Passwörtern, da Passwörter oftmals erraten werden können (z.B. sog. Wörterbuch-Angriffe). Deshalb könnte beim Vorliegen einer Smartcard-Authentifizierung dem Nutzer der Zugriff auf besonders sensible Datensatztypen gewährt werden.

Für die Zeit als Kontextparameter sind auch die verschiedenen Zeitzonen zu berücksichtigen. Mit diesem Kontextparameter kann z.B. verhindert werden, dass ein Nutzer sensible Geschäftsdokumente außerhalb der üblichen Geschäftszeiten ändert. Da für die Bestimmung der

Zeitzone auf die Ortung zurückgegriffen werden muss, ist ein Kontext-Parameter eine Eingangsgröße für die Ermittlung eines anderen Kontext-Parameters.

Die Termine eines Nutzers können über seinen vom System verwalteten Terminkalender ausgewertet werden. So kann beispielsweise verhindert werden, dass ein im Urlaub befindlicher Mitarbeiter vom System verwaltete Informationen verändert oder dass während des Termins bei einem bestimmten Kunden unbeabsichtigt auf Dokumente von einem anderen Kunden (der evtl. ein Mitbewerber des gerade besuchten Kunden ist) zugegriffen wird.

Die praktische Umsetzung des Datenmodells für Zugriffskontrolle und der Kontext-Schalter wurde von den Partnern auf der Basis der Anwendung des CodeMeter DRM-System evaluiert.

Das CodeMeter-Lizensierungssystem und die Abbildungsmöglichkeiten auf das Datenmodell wurden untersucht und auf die Einsatzmöglichkeiten des nPA erweitert. Es ergaben sich neue Möglichkeiten zur Anwendung des nPAs bezüglich einer geräteunabhängigen Nutzung der Ausweisfunktion innerhalb des CodeMeter-DRM-Systems. Konzepte für Bindungsmöglichkeiten von CodeMeterAct an Merkmale des nPAs wurden im Hinblick auf praktisch anwendbare Szenarien untersucht.

## **2.6 BACKEND-INTEGRATION**

Der Inhalt dieses Arbeitspaketes war die Integration der bestehenden stationären Unternehmenssysteme („Legacy-Systeme“) in die Gesamtarchitektur. In der Entwicklungsphase 1 wurde der CAS Open Server eine modulare Authentifizierungs- und Autorisierungsarchitektur sowie die Fähigkeit zur Anbindung von Legacy-Systemen im Unternehmensbackend erweitert. Damit wurde die angestrebte sichere Bündelung der darüber bereitgestellten Dienste realisiert. In der zweiten Phase des Arbeitspaketes wurde ein Demonstrator erstellt, der die vom Gateway umgesetzten Mechanismen zur Anbindung einer Legacy-Applikation nutzt.

## **2.7 INTEGRATION HARDWARE-TOKEN**

Die Weiterentwicklung der CodeMeter-Runtime im Zusammenspiel mit dem Browser und dem clientseitigen Proxy-Server wurde durchgeführt. Die Optionen für eine Integration von eID-Cards (z.B. kontaktbehaftet) für CodeMeter-Anwendungen mit einer generischen eCard-API wurden untersucht. Die bisher verwendete AusweisApp vom Hersteller OpenLimit bietet jedoch derzeit keine Anwendungsmöglichkeit. Daher wurden diese Optionen zur Integration von 3rd Party eID-Token nicht weiter verfolgt.

Der Anschluss des CodeMeter Authentifizierungs- und Lizenzmanagementservers an den eID-Server von ePA-Connect wurde auf Basis des bereitgestellten Testzertifikats für Wibu als Dienstanbieter ermöglicht. ePA-Connect stellte die erforderlichen Libraries (Komponenten für Protokoll-Stack, SAML kompatibel) bereit, die zur gesicherten Kommunikation mit dem eID-Server erforderlich sind. Das CodeMeter-Lizenzmanagement wurde als Webanwendung mit der eID-Serveranwendung

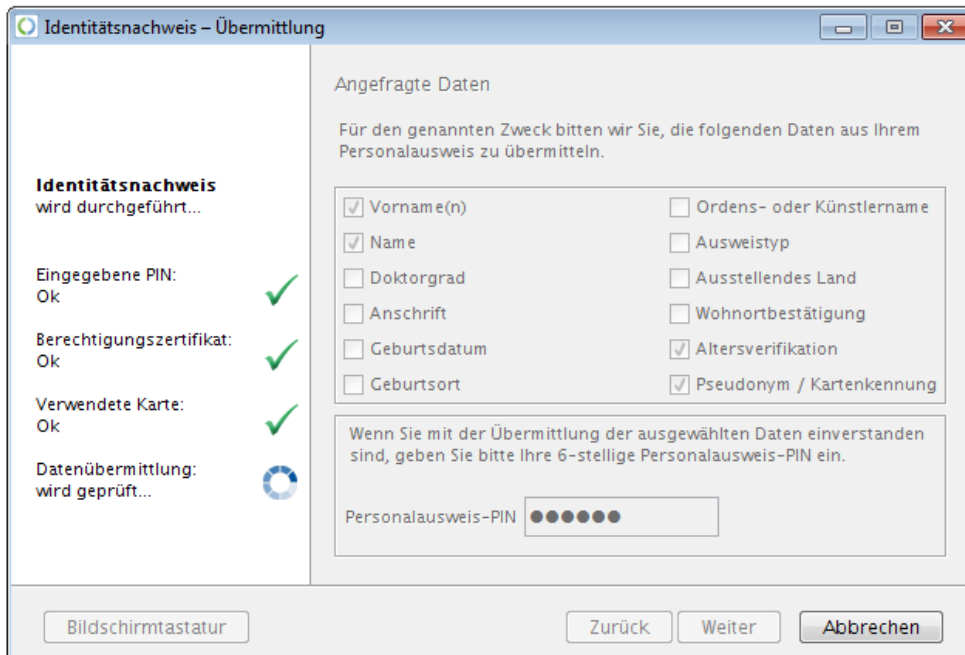
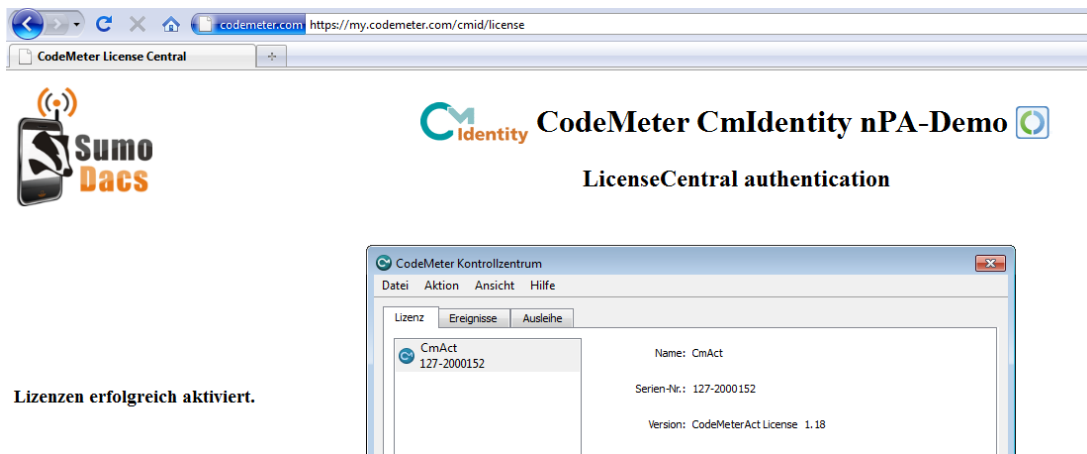


Abbildung 9: Screenshot Identitätsnachweis mit nPA

integriert. Ein erster Demonstrator zum Auslesen der nPA-Datenfelder und zur weiteren Verwendung im Lizenzmanagement wurde erstellt (siehe Darstellung Übersicht nPA-Demonstrator).



**Lizenzen erfolgreich aktiviert.**

Abbildung 10: Screenshot des nPA-Demonstrators, nPA und Lizenzaktivierung mit LicenseCentral

In den obigen Screenshots sind die AusweisApp mit den auszulesenden nPA-Merkmalen und die CodeMeterAct Lizenzdatei dargestellt. Im nachfolgenden Diagramm sind für den erstellten Demonstrator die Funktionsblöcke und die Prozessabläufe skizziert. Zuerst läuft die Authentifizierung mit dem nPA und dem eID-Server und anschließend erfolgt in der zweiten Phase die Bereitstellung der Daten für die Webseite. Der Reverse-Proxy organisiert die Kommunikation mit dem Servlet und dem Browser. Untenstehende Abbildung zeigt die Kommunikationsschritte für die Authentifizierung mit dem eID-Service

### Übersicht nPA-Demonstrator

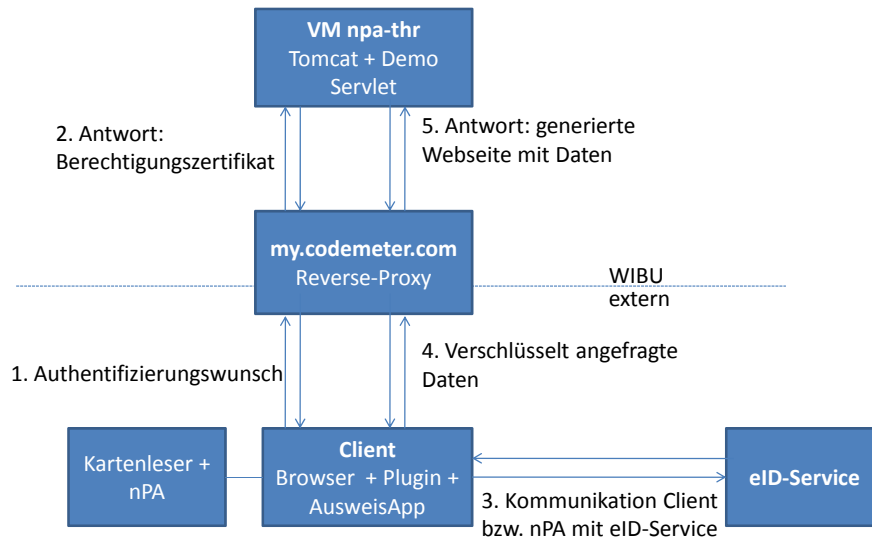


Abbildung 11: Übersicht nPA-Demonstrator, Reverse Proxy (http-Proxy)

## 2.8 IMPLEMENTIERUNG MOBILE CLIENTS

Die Entwicklungsarbeiten für die mobilen Clients, (zwei Klassen von mobilen Endgeräten, „Ultra Mobile PCs“ und „Smart Device“) unterschieden zu den jeweils in Frage kommenden Betriebssystemen wurden durchgeführt. Die neuen Betriebssysteme von Windows und MacOS standen bei den browserbasierenden Entwicklungen im Vordergrund. Smartphones können wegen der teilweise bestehenden, technischen Einschränkungen für die CodeMeter-Runtime derzeit noch nicht unterstützt werden. Insoweit erstreckten sich die Entwicklungsarbeiten in erster Linie auf mobile PCs, für die auch die Anwendung des nPA mit portablen Lesern in Betracht kam. Für den mobilen Smartphone-Bereich stand für die Integration in die SumoDacs Infrastruktur lediglich ein Smartphone mit Windows Mobile 6.5 zur Verfügung. Als Zugangstoken dient eine CmCard/μSD. Die Netzwerkkommunikation, die Proxy-Implementierung und die Kommunikation mit dem Browser konnte für eine prototypische Zugriffslösung, basierenden SumoDacs Zwei-Faktor Authentifizierung in die mobile Anwendung „CAS Mobile Access“, bereitgestellt werden. Aus Gründen der drastisch veränderten Marktperspektive wurden die Entwicklungsarbeiten allerdings nicht im ursprünglich geplanten Umfang für die derzeit am Markt verfügbaren mobilen Betriebssysteme durchgeführt.

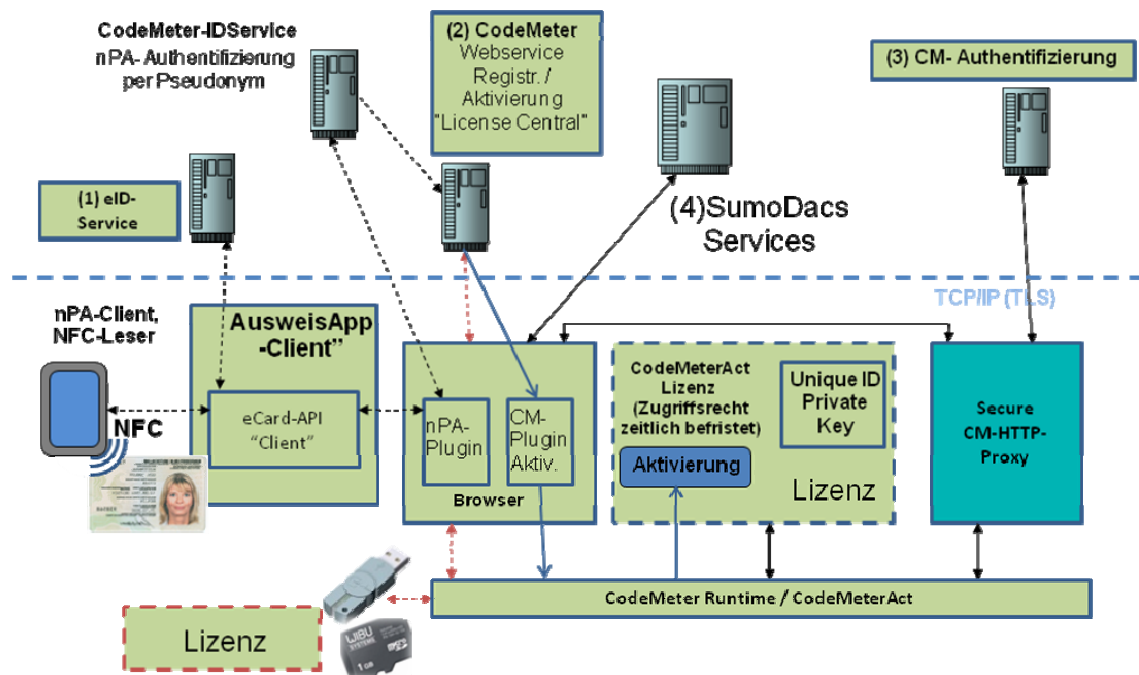


Abbildung 12: Webbasierter stationärer/mobiler Client: AusweisApp, Browser und http-Proxy zur Unterstützung von nPA und CodeMeterAct sowie von CodeMeter-Token (Stick und microSD)

Die generell anwendbare unique ID eines Tokens verbunden mit dem nicht zugänglichen „Private Key“ dient zur eindeutigen Authentifizierung mit dem Backend-Server in der Anwendung eines asymmetrischen Verschlüsselungsverfahrens. Anstelle des Hardware-Tokens stellt bei einem softwarebasierten, aktivierten Token mit CodeMeterAct stattdessen der Lizenzcontainer eine „Unique ID“ und den Schlüssel für den Authentifizierungsprozess bereit. Der webbasierte Authentifizierungsvorgang läuft dann jeweils über den secure CM-http-Proxy (Reverse-Proxy).

Eine besondere Herausforderung bei Verwendung drahtloser Datenkommunikation ist die Berücksichtigung von ungeplanten Kommunikationsabbrüchen (z.B. „Funkloch“). Die SumoDacs-Architektur sieht deshalb vor, dass mobile Endgeräte auch teilweise autark arbeiten können, also einen begrenzten eigenen Datenbestand vorhalten können. Zum Abgleich dieses Datenbestandes wird auf beiden Seiten eine Synchronisationskomponente benötigt. Auf einem mobilen Endgerät vorgehaltene („gecachte“) Daten werden zusätzlich verschlüsselt, damit beim Verlust des Endgerätes die Daten nicht Unbefugten in die Hände fallen. Dazu wurde ein performantes Verfahren zur verschlüsselten Speicherung heruntergeladener Daten entwickelt, das keine Anpassung des Betriebssystemkerns erfordert und mit Hilfe des Hardware-Tokens eine sichere Speicherung auf Applikationsebene realisiert. Bei Verlust des Hardware-Tokens ist es dem Sicherheitsserver möglich, ein neues, äquivalentes Token zu programmieren, mit dessen Hilfe die verschlüsselten Daten auf dem Smartphone gerettet werden können.

Die entsprechenden unterstützenden Sicherheitsfunktionen des Proxy-Servers zur Kommunikation mit dem Backend-System und dem Browser sowie die Mechanismen zur Synchronisation von gecachten Daten und Dokumenten wurden für den mobilen Client prototypisch entwickelt.

Die im Arbeitspaket zunächst geplanten Arbeiten für die Integration eines spezifischen mobilen Smartphone-Clients mit nPA-Lesefähigkeiten konnten nicht durchgeführt werden, weil derzeit kein auf dem Markt erhältliches Smartphone existiert, welches die gerätetechnischen Voraussetzungen zum Lesen des nPA anbieten könnte. Dies liegt unter anderem an der besonderen Anforderung an das Datenvolumen, welches bei der Kommunikation des nPA mit dem Leser über die standardisierte Luftschnittstelle NFC (Near Field Communication, Air Interface ISO/IEC 14443) zu übertragen ist. Obwohl eine Reihe von NFC-fähigen Smartphones mittlerweile die standardisierte Funkschnittstelle unterstützen kann, scheitern diese bereits an der Übertragung des spezifischen Datagramms. Aspekte der Zertifizierbarkeit der Leserfunktion in einem Massenmarktprodukt wie dem Smartphone stellen neben der Bewältigung des Übertragungsprotokolls noch ein weiteres technisches Problem für einen Gerätehersteller dar.

## 2.9 VORGEHENSMODELL

Das Vorgehen bei der Entwicklung der Funktionalitäten von SumoDacs wurde in einem Vorgehensmodell verallgemeinert. Für eine bessere Verständlichkeit wurden aus dem Gesamtvorgehensmodell (Abbildung 13) drei Teilvorgehensmodelle herausgelöst und weiter detailliert (Berechtigungsmodell, Backend, mobiler Client).

Zu Beginn des neuen Projektes müssen die Anforderungen analysiert werden (*Phase Analyse*). Hier entscheidet sich, ob das Zielsystem mit den Anforderungen grundlegend realisiert werden kann, ob Anforderungen modifiziert werden müssen oder ob das Vorhaben gänzlich nicht machbar ist. Nachdem die Machbarkeit positiv bewertet wurde und die Anforderungen feststehen, sind die Bedrohungen zu analysieren, die sich aus der zukünftigen mobilen Anbindung an das System ergeben. Auch hier kann es notwendig sein, das Vorhaben abzubrechen, falls die mobile Anbindung zu viele, nicht beherrschbare Sicherheitsprobleme aufwirft.

Sind die Anforderungen realisierbar und die Bedrohungen beherrschbar, kann mit der Entwicklung der mobilen Lösung begonnen werden (*Phase Entwurf*). Parallel können dabei folgende Aktivitäten ablaufen: Das Erstellen von Gesamtarchitektur, Kommunikationsprotokollen, kryptografischen Protokollen und des Berechtigungsmodells. Je nach konkretem Einzelfall können (Teil-)Ergebnisse der verschiedenen Aktivitäten aufeinander aufbauen oder teilweise sequenziell abgearbeitet werden. Im Anschluss werden in der *Phase Realisierung* die in der vorherigen Phase entwickelten Architekturen, Modelle und Protokolle softwaretechnisch umgesetzt und in das Backend integriert. Parallel dazu kann der mobile Client entwickelt und implementiert werden. Sobald alle system-relevanten Bestandteile zusammengefügt sind, kann das Gesamtsystem getestet werden (*Phase Testen*). Sofern evtl. vorhanden Unstimmigkeiten behoben sind, kann zur Phase Pilotbetrieb übergegangen werden, in welcher das entwickelte System eine Zeit lang unter realen Bedingungen verwendet wird. Sollten dabei Probleme auftreten, so ist an den entsprechenden Stellen nachzubessern. Schließlich wird das System vollständig eingeführt (*Phase Einführung*). In Abhängigkeit von bereits bestehenden Systemen, der Neuentwicklung, etwaigen Managementvorgaben und weiteren Faktoren kann die Einführung auf verschiedene Weise erfolgen. Möglich ist beispielsweise eine Umstellung zu einem bestimmten Stichtag, das heißt, zu diesem Datum wird die Neuentwicklung in Betrieb genommen und ein bestehendes Altsystem, welches durch das neue ersetzt wird, dabei abgeschaltet. Um einen abrupten Umstieg zu vermeiden, kann - sofern dies die Lösung erlaubt - das neue System auch teilweise über mehrere Schritte oder Stufen eingeführt werden. Auch kann es in manchen Situationen sinnvoll sein, zwei Systeme parallel eine gewisse Zeit zu betreiben, bis etwa das neu entwickelte System ohne Probleme läuft und die Mitarbeiter damit zurechtkommen. Wurde ein bestehendes System um Funktionalitäten erweitert oder verbessert, so kann dies auch als Umstellung auf eine höhere gesehen werden.



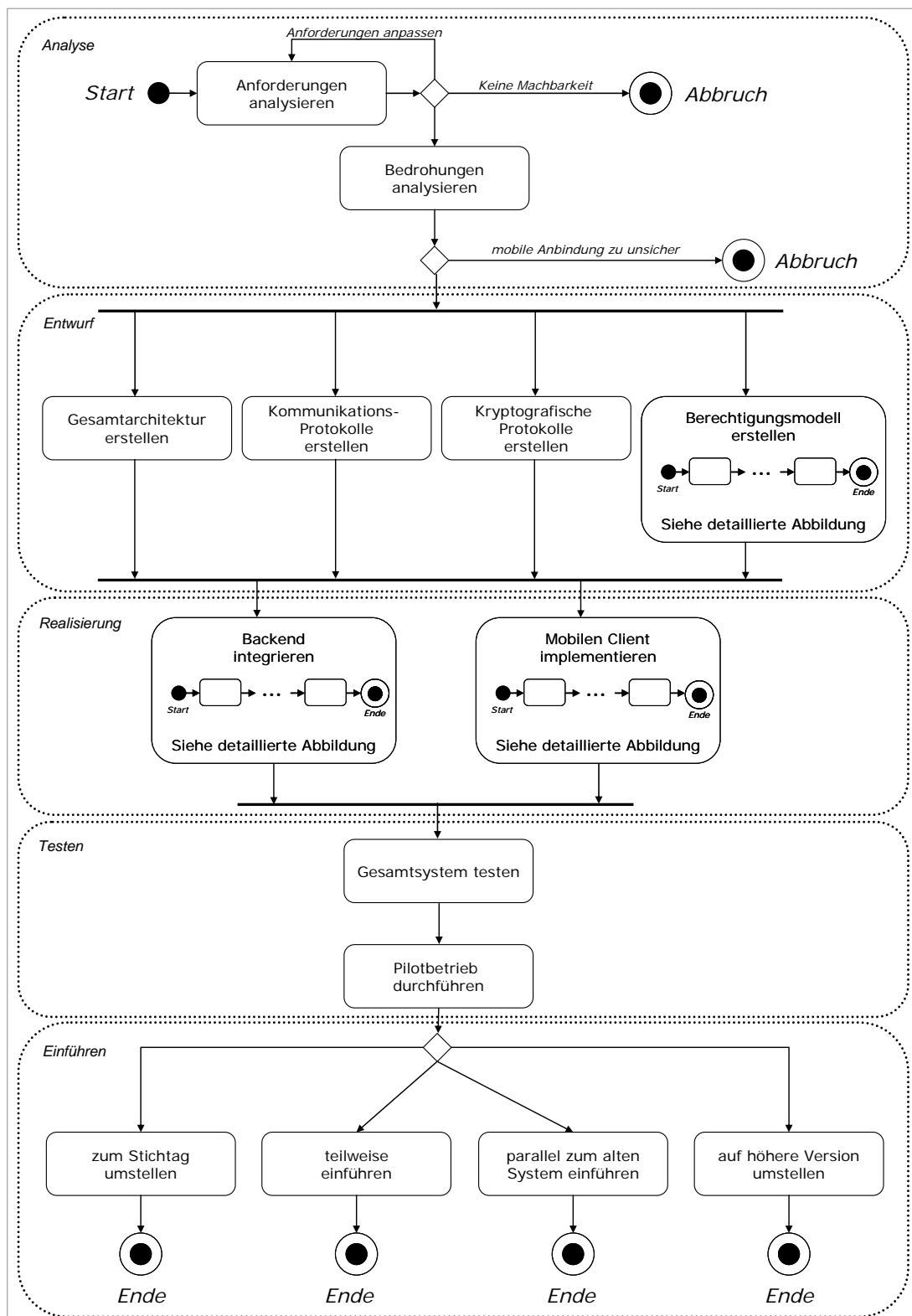


Abbildung 13: Gesamtvorgehensmodell.

Eine wichtige Aufgabe der Entwurfsphase ist die Erstellung des Berechtigungsmodells (Abbildung 14), das auf Grundlage der ermittelten Anforderungen, also der Erfordernisse, Möglichkeiten und Hindernisse, entwickelt wird. Ist noch kein Berechtigungsmodell vorhanden, so können parallel das Grundmodell erstellt und Kontextparameter identifiziert werden. Für den Entwurf des Grundmodells werden betriebliche Dokumentationen verwendet. Das erstellte Grundmodell muss mit den bestehenden Implementierungen abgeglichen und gegebenenfalls Grundmodell oder Implementierungen angepasst werden. Parallel dazu werden die Kontextparameter untersucht. Zunächst werden die möglichen Kontextparameter identifiziert und anschließend in einem weiteren Schritt bewertet. Dieser Vorgang kann mehrmals wiederholt werden, etwa bis alle notwendigen Parameter bestimmt sind. Um Kontextschalter zu ermitteln, muss ein Berechtigungsmodell vorliegen, das heißt, es kann bereits bestehen oder wurde parallel - wie hier beschrieben - erstellt. Darauf aufbauend können die möglichen Andockstellen für das Einbinden von Kontextschaltern identifiziert werden. Im nächsten Schritt werden in Abhängigkeit vom Berechtigungsmodell und den zur Verfügung stehenden Kontextparametern die umzusetzenden Kontextschalter definiert. Damit steht das Berechtigungsmodell zur Verfügung, kann in das Gesamtmodell eingearbeitet und in der nächsten Phase umgesetzt werden.

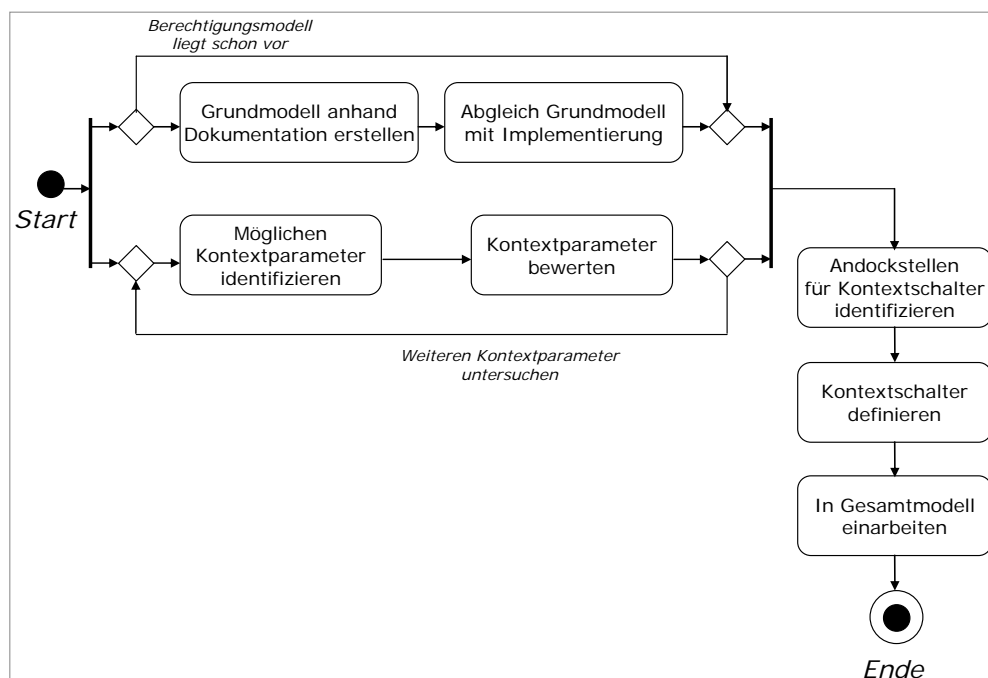


Abbildung 14: Teilvorgehensmodell Berechtigung

Im Anschluss an die Entwurfsphase folgt die Realisierung (Abbildung 15). Hier werden parallel die neuen Architekturen, Modelle und Protokolle umgesetzt und in das Backend integriert sowie der mobile Client implementiert. Aufbauend auf den bestehenden Architekturen wird bei der Backend-Integration zunächst die Geschäftslogik angepasst und bei Bedarf ergänzt. Für die Integration ist es unerlässlich die Schnittstellen zwischen bestehenden Systemen und der neuen bzw. erweiterten Anwendung zu definieren und im Detail zu spezifizieren (Feinspezifikation). Erst dann kann die tatsächliche Implementierung erfolgen. Dabei können die Schritte Anbinden der Schnittstellen, Einbinden der kryptografischen Protokolle, Integration des Security-Token und das Umsetzen des

Berechtigungsmodells in der Regel weitgehend parallel ablaufen. Gegebenenfalls bedingen sich einzelne Elemente dieser Schritte oder bauen ganze Schritte der Implementierung aufeinander auf. Dies ist jedoch vom Einzelfall und der konkreten Umsetzung abhängig.

Schließlich wird das System auf den Gesamttest vorbereitet. Der Systemtest und der Pilotbetrieb stehen vor der endgültigen Systemeinführung und sind im Gesamtvorgehensmodell zu finden.

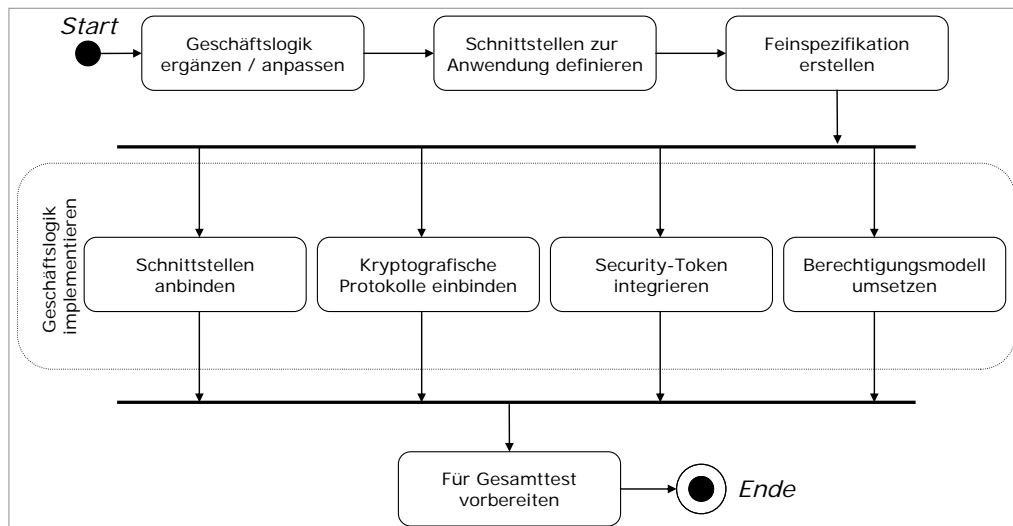


Abbildung 15: Teilmodell Backend Integration.

Parallel zur Backend-Integration wird der mobile Client implementiert (ggfs. auch mehrere). Im Wesentlichen besteht das Vorgehen dabei aus den in Abbildung 16 dargestellten Schritten: In der Teilarchitektur werden alle notwendigen bzw. eventuell möglichen Funktionalitäten, Abläufe oder auch nicht-funktionale Eigenschaften festgelegt, welche dann in eine Feinspezifikation überführt werden. Anschließend erfolgt die Implementierung, indem die kryptografischen Protokolle eingebunden und gleichzeitig das Security-Token integriert werden.

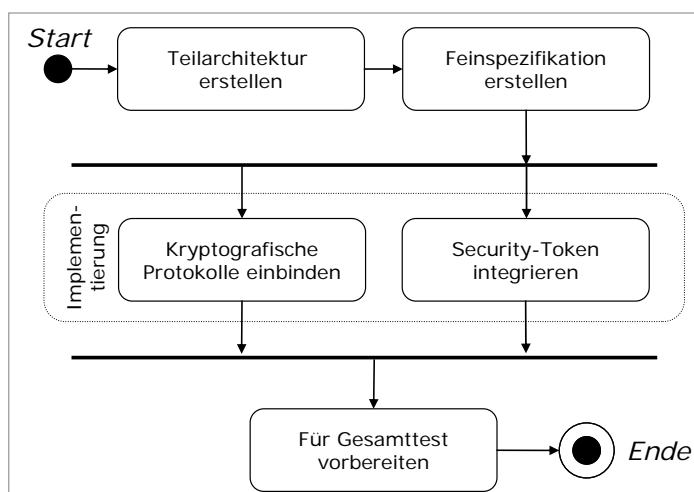


Abbildung 16: Teilmodell Mobile Client Implementierung.



Die beiden Aktivitäten der Implementierung ähneln denen der Backend-Integration, da beide Bereiche einen Teil der erweiterten Sicherheitslösung darstellen. Das Teilvorgehensmodell schließt ebenfalls mit der Vorbereitung auf den Gesamtsystemtest ab.

## 2.10 WISSENSCHAFTLICHE EVALUATION

Der Evaluation zugrunde lagen Szenarien, welche vier Tage eines Verkaufsdirektors darstellten. Zu jedem Tag (also zu jedem Szenario) gab es eine Situationsbeschreibung und von den Probanden durchzuführende Aufgaben. Nach jedem Szenario wurden je drei (gleiche) Fragen gestellt und am Ende war ein Gesamtfragebogen auszufüllen.

Die Ergebnisse der Evaluation der Benutzerstudie zeigen auf, dass die gefühlte Sicherheit sich entsprechend mit der besseren Sicherheit durch die SumoDacs-Lösung erhöht. Die Evaluation zeigt auch, dass die SumoDacs-Lösung eine hohe Gebrauchstauglichkeit aufweist. Es ist sehr positiv zu bewerten, dass die Sicherheitsverbesserung angenommen wird. Im Detail werden einige Ergebnisse nachfolgend beschrieben.

Die gefühlte Sicherheit wurde mit der Frage "Insgesamt fühle ich mich sicher bei der Verwendung der Security-Token." allgemein erfasst. Weiter wurde im Detail nachgefragt, ob sich die Probanden mit dem Security-Token bei der Nutzung der Anwendung sicherer als ohne Token fühlen. Werden die höchsten beiden Skalenwerte (also 7 „stimme zu“ und 6) der sieben Stufen zusammengefasst, so ergibt sich, dass sich rund zwei Drittel der Befragten mit der Verwendung des Security-Token sicherer fühlen als ohne.

Wird der TabletPC verloren oder gestohlen und ist der berechtigte Nutzer weiterhin im Besitz des Security-Token, ist objektiv die Sicherheit weiterhin gegeben, denn ohne den Token sind die noch auf dem Gerät vorhandenen Daten nutzlos. Die gefühlte Sicherheit lag nur ein wenig darunter, sodass festgehalten werden kann, dass sich die Probanden tatsächlich sicherer fühlen, wenn sie einen Security-Token nutzen.

Neben der Perceived Security wurde die Usability der Sicherheitstoken untersucht. Bei der Verwendung von Sicherheitsmechanismen ist es immer wichtig, dass auch die Nutzer, d.h. die von den jeweiligen Mechanismen Betroffenen, damit gut zu Recht kommen. Andernfalls werden sonst Mittel und Wege gefunden, umständliche und wenig gebrauchstaugliche Methoden zu umgehen. Im Ergebnis zeigte sich, dass die Verwendung eines Token eine handhabbare Methode ist, eine sehr gute Sicherheit zu gewährleisten, was sich positiv auf die Usability und somit auch auf die tatsächliche Sicherheit auswirkt. Auch wurde die Ausführung der Anwendung durch den Token weder auf dem PC noch auf dem TabletPC merklich beeinflusst. Bei beiden Geräten reagierte die Anwendung schnell.

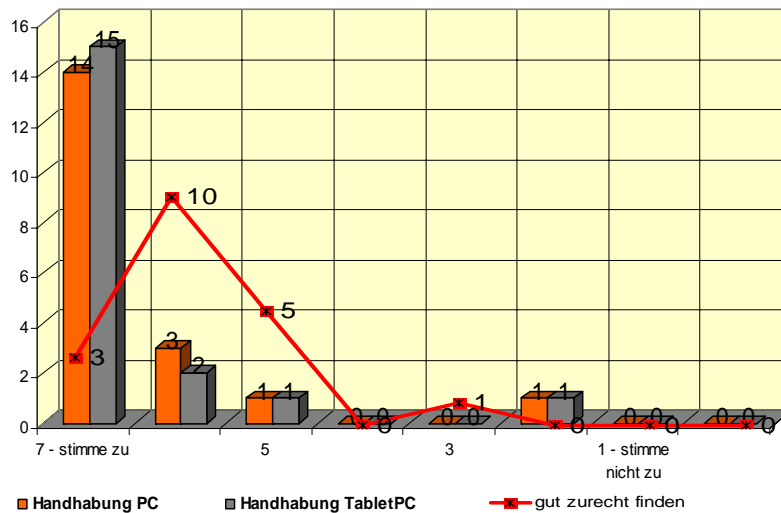


Abbildung 17: Handhabung des Token mit PC / TabletPC im Vergleich zum Zurechtfinden in der Anwendung

Wird die Handhabung der Security-Token mit der sonstigen Handhabung der Anwendung verglichen, so zeigt sich, dass der Token besonders durch seine leichte Verwendung gekennzeichnet ist. Die Nutzung des Token wird insgesamt als einfacher angesehen als die der Anwendung. Dies ergibt sich daraus, dass zum Erreichen einer hohen Sicherheit aus Nutzersicht lediglich eine Hardware-Komponente angesteckt wird. Sicherheitsmechanismen haben oft das Problem, dass sie bei hoher Sicherheit eine geringe Usability aufweisen. Aufgrund der Einfachheit in der Handhabung der Token sind die Nutzer weniger bestrebt, diesen Sicherheitsmechanismus zu umgehen. Aus Sicht des Nutzers ist eine Anwendung wie CAS PIA in der Nutzung komplexer als ein ansteckbarer Sicherheitstoken. Somit ist es leichter sich mit der Nutzung des Token vertraut zu machen als mit der Anwendung im Szenario umzugehen. Die Anwendung, besonders in der PC-Variante, erfordert einen höheren Aufwand um ihre Möglichkeiten kennen und verwenden zu lernen als das einfache Anstecken des Token.

Anhand des Fragebogens nach jedem Szenario konnte festgestellt werden, dass es Lerneffekte gab. So ist zu sehen, dass je mehr die Anwendung genutzt wurde, desto einfacher fanden sich die Probanden zurecht. Ebenso stieg von Szenario zu Szenario die Zufriedenheit bezüglich der benötigten Zeit, die für die Aufgabenlösung benötigt wurde. Es kann festgehalten werden, dass je mehr die Anwendung genutzt wurde, desto schneller konnten die Aufgaben gelöst werden.

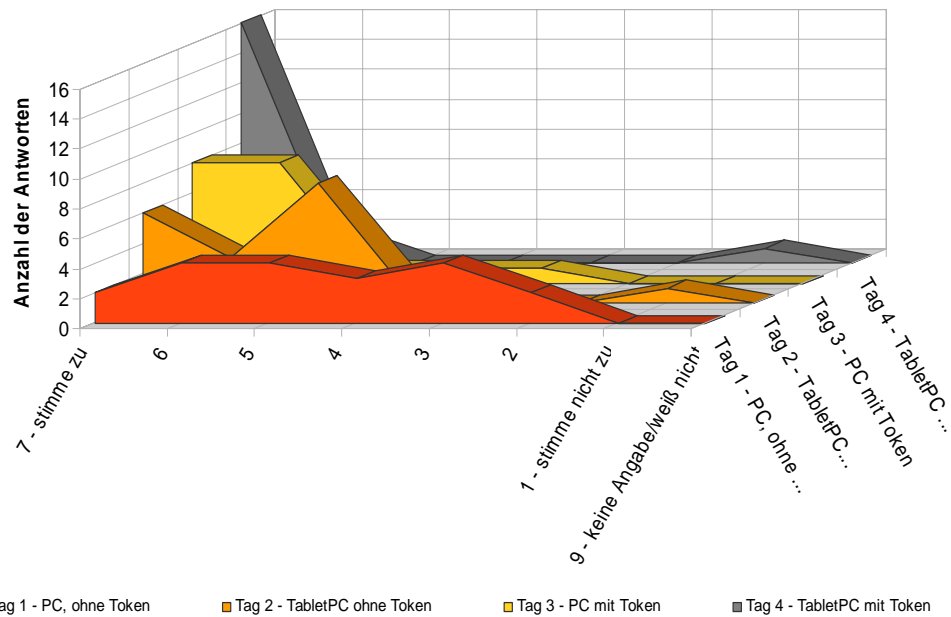


Abbildung 18: Vergleich der Szenarien-Tage bzgl. Einfachheit

Auch ein Vergleich der Häufigkeit der in Anspruch genommenen Hilfestellung durch den Versuchsleiter zeigt, dass es Lerneffekte gab. Im Einzelnen lässt sich feststellen, dass die Hilfestellung bei Tag 3 und Tag 4 weniger nötig gegenüber Tag 1 und Tag 2 war. Darüber hinaus zeigte sich, dass mehr Hilfe bei der Verwendung des stationären PC verlangt wurde als beim TabletPC. Dies kann dadurch erklärt werden, dass zum einen zunächst die PC-Variante verwendet wurde und anschließend der TabletPC, sodass auch hier Lerneffekte eine Rolle spielen. Zum anderen kann es darin begründet sein, dass die Anwendung auf dem PC umfangreicher ist und mehr Möglichkeiten bietet als die auf dem TabletPC. Bei letzterer werden lediglich die für die aktuelle Verwendung relevanten Dinge angezeigt. Diese Beschränkung führt dazu, dass die Anwendung einfacher zu nutzen ist.

### **3 NOTWENDIGKEIT UND ANGEMESSENHEIT DER GELEISTETEN ARBEITEN**

SumoDacs weist einen innovativen Charakter auf, in dem die 3 Zonen-Architektur in einem neuen Ansatz zur Integration von Authentifizierung und Erteilung von Zugriffsrechten zu softwarebasierten Services prototypisch umgesetzt wurde. Die Integration der Legacy-Anwendungen über die Backend-Plattform basierend auf PIA und CAS Open mit den browserbasierten Clients stellte eine technologische Herausforderung dar, insbesondere auch unter dem Gesichtspunkt der Integration der Hardware-Token in eine weitgehend offene und modulare Architektur sowohl server- als auch clientseitig.

Die Integration des nPA betreffend war ein neues Konzept zu finden, wie Authentifizierung und Zugriffsberechtigung neben den anderen Methoden wie Username/Passwort oder SSO am zweckmäßigsten zu integrieren war, ohne den verfolgten Ansatz der Modularität und Austauschbarkeit von Komponenten zu verlassen. Die Umsetzung der Option, den nPA als Token für den Zugang mit Berechtigungen zu Legacy-Anwendungen benutzerfreundlich zu integrieren und einzusetzen, war eine der technologischen Herausforderungen, die im Laufe des Projekts zu meistern war.

Die Auseinandersetzung mit der Entwicklung der neuen mobilen Plattformen war ein weiteres Thema während der Entwicklungsarbeiten für den mobilen Client. Durch die rasche Veränderung der Technologien und Plattformen im Smartphone- und Tablet-Bereich gab es auch hier Herausforderungen, mit den Innovationszyklen mitzuhalten. Die Arbeiten hierzu waren notwendig, um zu erkennen, wie sich mobile Betriebssysteme weiterentwickeln und welche Rolle browserbasierte Lösungen zukünftig spielen werden, wenn standardisierte HTML5-Browser zur Verfügung stehen.

Die obigen Ausführungen zeigen, dass die Arbeiten in den genannten Entwicklungsbereichen sinnvoll und notwendig waren, um ein sicheres und offenes Dreizonenmodell im Konzept und auch prototypisch zu realisieren. Auch im wissenschaftlichen Bereich ergaben sich Forschungsfelder, in den intensiv geforscht wurde. In den beschriebenen Arbeitspaketen, siehe z. B. Datenmodell für Zugriffskontrolle, wurden wichtige Erkenntnisse gewonnen, die in die konkrete Umsetzung der Architektur einfließen. Die Integration der kontextsensitiven Zugriffsmechanismen erforderte die Implementierung innovativer und performanter Datenzugriffsmethoden. Daraus resultierender Entwicklungsaufwand verbunden mit technischem Risiko rechtfertigen die geleisteten Arbeiten.

Insgesamt versprechen sich die Projektteilnehmer, hier insbesondere die Industriepartner, von den entwickelten Lösungen eine direkte Verbesserung ihrer Marktposition und der Wettbewerbsfähigkeit. Von daher waren die geleisteten Arbeiten ein notwendiges Investment, den künftigen Herausforderungen bedingt durch den immer schneller werdenden technologischen Wandel besser begegnen zu können.

### **4 VERWERTBARKEIT DER ERGEBNISSE**

Im nachfolgenden Schaubild sind die Phasen für die anschließende Weiterentwicklung einer CAS Open Version 0 (Plattform as a Service, PaaS) in 3 parallel verlaufenden Zeitsträngen skizziert.



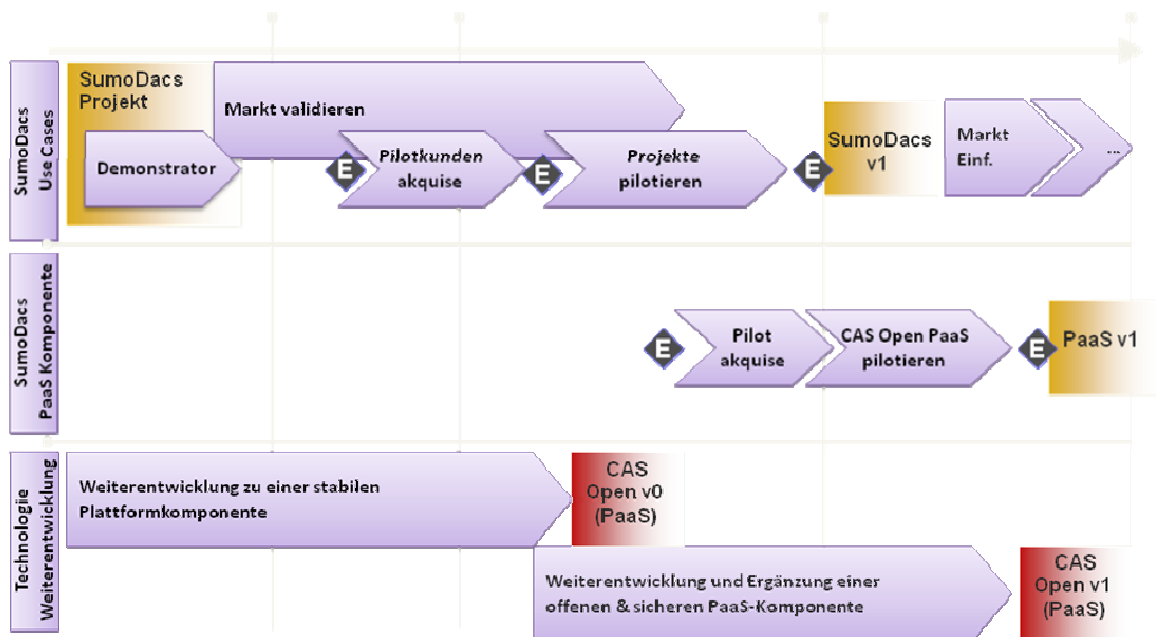


Abbildung 19 - Weiterentwicklung von CAS Open zu einer ‚Platform as a Service‘ und Markteinführung

Für das Umsetzen des Sumodacs-Sicherheitskonzeptes in ein marktfähiges Produkt auf der Basis einer offenen und sicheren PaaS wurden im Laufe des Projekts folgende Punkte als essenziell identifiziert:

1. Anpassung der Entwicklung zu einer offenen, erweiterbaren Authentifizierungs- und Sicherheitsinfrastruktur, sowie passende Integration in CAS Open, wobei insbesondere zusätzliche Authentifizierungsmerkmale für jeden Nutzer hinterlegbar und zur Anmeldung nutzbar sein sollen
2. Nutzung der vorhandenen Infrastruktur für die Implementierung einer hardwaregestützten Authentifizierung (CodeMeter-Token, Security-Proxy,...), sowohl für Desktop-/Browser-Szenarien als auch auf Mobilgeräten
3. Nutzung der Infrastruktur für die Implementierung einer OpenID-basierten Authentifizierung
4. Nutzung der Infrastruktur für kontextabhängige Security

Alle genannten Punkte wurden im Projekt adressiert und durch die Entwicklung entsprechender Konzepte und, mit Ausnahme von Punkt 4, durch prototypische Implementierungen auf Basis der in Entwicklung hin zu einer Version 0 befindlichen PaaS-Lösung CAS Open realisiert. Dank dieses erfolgreichen Projektverlaufs können die im Projekt gewonnenen Erkenntnisse zur Gestaltung einer sicheren und gleichzeitig flexiblen PaaS-Lösung unmittelbar im Rahmen der technologischen Weiterentwicklung von CAS Open (siehe Abbildung 19) verwertet werden.

Der im Rahmen des Projekts entwickelte Demonstrator zeigt auf eindrucksvolle Art und Weise die praktische Einsetzbarkeit und Relevanz der in SumoDacs entwickelten Ansätze und der erzielten Projektergebnisse. Er stellt damit aus Sicht der CAS Software AG eine ideale Grundlage für in Abbildung 19 im Zeitstrang "SumoDacs Use Cases" abgebildeten Schritte der Validierung des Marktes und die angestrebte Pilotkundenakquise dar.

Die Gesamtlösung wird basierend auf den Entwicklungsergebnissen von SumoDacs vom Projektpartner CAS gemäß dem obigen Einführungsplan für das CAS vermarktet. Wibu-Systems liefert die entwickelten Hard- und Softwarekomponenten für die Sicherheitsanwendung entweder an CAS und/oder direkt an den Käufer, soweit die eigenentwickelten Komponenten zur Anwendung kommen. Für den Anwendungsfall des Einsatzes des nPA ist derzeit nur eine Testbetriebsvariante in einer Authentifizierungs- und Lizenzmanagementlösung vorgesehen. Damit können Teststellungen für einen Pilotbetrieb beim Kunden unterstützt werden. Es bestehen aus technischer und kommerzieller Sicht verschiedene Optionen den Regelbetrieb um eine nPA-Authentifizierungslösung bei einem externen Dienstleister zu hosten. Wibu-Systems plant derzeit nicht, als zertifizierter Dienstleister für nPA-Kundenlösungen aufzutreten. Die weitere Erschließung des Kundenpotentials hängt auch von der generellen Entwicklung des Marktes in Bezug auf eine breitere Akzeptanz des nPA ab.

Im Hinblick auf ein mögliches Pilotprojekt könnte sich eine Campuslösung im universitären Bereich als derzeit aussichtsreichstes Anwendungsszenario erweisen. Logischer Zugang (zu IT-Ressourcen) und in gewissen Grenzen auch physische Zugangskontrolle zu Gebäuden und sonstigen Campusressourcen ließen sich auf der Basis der Weiterentwicklung des SumoDacs-Konzeptes realisieren. Es wird darüber hinaus erwartet, dass sich mittelfristig Impulse für weitere Anwendungen in öffentlichen Institutionen ergeben werden. Das Gesamtkonzept von SumoDacs lässt sich künftig sehr gut an einzelne Bedarfsfälle anpassen, in denen der nPA als Teilkomponente in einer gemischten Anwendung mit CodeMeter-Token Vorteile bieten kann.

#### Verwertung von Teilergebnissen:

Für Wibu-Systems ergeben sich Perspektiven in der Verwertung von Teilergebnissen. Unabhängig von der Option einer Gesamtverwertung, wie oben beschrieben, bietet Wibu-Systems entwickelte Teilkomponenten an interessierte Kunden, die neben einer Softwareschutzanwendung eine spezielle Token-Lösung in ein eigenentwickeltes Identitäts- und Access Managementsystem integrieren wollen. Identity-Management und Zugriffsteuerung können grundsätzlich beide durch Anwendung desselben Token oder aber auch durch getrennte Verwendung zweier Token (Trennung in Authentifizierung und Autorisierung/Zugang) implementiert werden. Zum angestammten Geschäftsfeld Softwareschutz kommen dann die webbasierten Access-Methoden als komplementäre Sicherheitsanwendungen hinzu.

Der mobile Endgeräte Markt könnte sich als ein weiteres Marktsegment erweisen, in denen die CodeMeter-Tokenlösungen auf Basis von Flashkarten zum Einsatz kommen, sobald die Weiterentwicklung des secure Proxy zur Unterstützung offener Betriebssysteme wie Android und Windows Phone 8 durchgeführt wurde.

## 5 FORTSCHRITTE AUF DEM GEBIET DES VORHABENS

Im Rückblick auf die zwischenzeitlich gemachten Fortschritte innerhalb der letzten zweieinhalb Jahre lassen sich auf den verschiedenen technologischen Gebieten, in den das Projekt angesiedelt war, bemerkenswerte Tendenzen feststellen:

Sowohl im Hard- als auch im Softwarebereich sind die technologischen Neuerungen von zum Teil neu in Erscheinung tretenden Unternehmen in erstaunlichem Maße vorangetrieben worden. Als bemerkenswertester Trend war die unvorhersehbare Entwicklung des mobilen Marksegments mit rasch expandierenden Kategorien von Smartphone und Tablets angetrieben durch Wettbewerb verbunden mit einer hohen Innovationsrate. Das Mobile Internet ist in dem betrachteten Zeitraum in globalem Maßstab zum Massenphänomen geworden. Entsprechend schnell mit der Steigerung der Prozessorleistungsfähigkeiten (Mehrkern- und Graphikprozessoren) haben sich die Betriebssystemplattformen gewandelt. Die Unterstützung von webbasierenden Anwendungen ist weiter in den Vordergrund gerückt und Speicherkapazitäten im GB-Bereich sind sowohl lokal als auch in entfernten Servern fast unbegrenzt verfügbar. Auch die mittlerweile installierte Bandbreite im mobilen Bereich nähert sich denen in Festnetzen. Daher sind alle Voraussetzungen auch geschaffen, dass der bisher auf dezentrales Desktop-Computing ausgerichtete Unternehmensarbeitsplatz um mobile Lösungen ergänzt wird. Webbasiertes Computing über Software as a Service (SaaS) und in einem weiteren Trend im Cloud-Computing begünstigen entsprechend zentralisierte und virtualisierte Infrastrukturen. Die Weiterentwicklung der Browser und deren zunehmende Bedeutung für Desktop-Computing sind ein Beleg dafür.

Die Smartcard-Technologie, ansonsten eher einem stetigen und gut vorhersehbaren Innovationszyklus folgend, hat von den Markttendenzen ebenfalls neue Impulse erfahren. Die NFC-Technik benötigt ein Secure Element, damit Transaktionen und Autorisierungen bei allen Geschäftsprozessen sicher abgewickelt werden können. Eine Vielzahl neuer Anwendungen mit kontaktlos token wird erwartet, nachdem Finanzdienstleister in großem Rahmen die neue Technik als embedded oder steckbare Variante einsetzen wollen.

Die Standardisierung für sichere Kernbereiche im OS, unterstützt durch Hardware-Funktionen (SoC), eröffnet Interoperabilität mit Browsern und webbasierten Anwendungen. Zu den standardisierten sicheren Elementen gehören SIM-Karten und microSD. Speziell der mobile Bereich wird damit zum Vorreiter für den Einzug von SEs in den Notebook- und den Desktopbereich. Die Anwendung von kontaktlos Karten und Mobiltelefonen beginnen als Zugangstoken im Unternehmensbereich derzeit in Pilotprojekten an Bedeutung zu gewinnen. Vor diesem Hintergrund war die Integration des nPA ein wichtiger Schritt, die neuen kontaktlostechnologien in einer SumoDacs-Lösung grundsätzlich unterstützen zu können.

Aus wissenschaftlicher Sicht gibt es einige Fortschritte im Bereich sicherer Zugriff auf Daten über ein nicht-vertrauenswürdiges Gerät. Im Rahmen des Secure Cloud Computing wurden unter den Stichworten „Searchable Encryption“ und „Functional Encryption“ einige Techniken entwickelt, die es ermöglichen, auf Daten zu suchen oder Daten zu verarbeiten, ohne diese zu entschlüsseln. Mit Hilfe dieser Techniken kann zusätzlich oder zusammen mit dem Hardware-Token die Sicherheit webbasierter Anwendungen immens erhöht werden. Auch auf dem Gebiet, kryptographische Maßnahmen mit sicheren Hardware-Tokens zu verbinden, gibt es einige Fortschritte, die sich allerdings größtenteils eher am Rande des Gebiets des Vorhabens bewegen.

Eine weitere Neuentwicklung im Bereich der Verschlüsselungsverfahren sind sogenannte attributbasierte Verschlüsselungen (Attribute Based Encryption, ABE), mit deren Hilfe es möglich ist, Daten kontextbasiert oder auch rollenbasiert zu entschlüsseln. ABE bietet die Möglichkeit, das Rechtemanagement direkt in die Verschlüsselung zu integrieren. Allerdings steht einem praktikablen Einsatz dieser Verfahren noch deren mangelnde Effizienz entgegen.

## **6 ERFOLGTE UND GEPLANTE VERÖFFENTLICHUNGEN**

*SumoDacs: Absicherung des mobilen Zugriffs auf Unternehmensanwendungen mit einer manipulationsresistenten Smartcard*

Das Projekt SumoDacs wurde auf dem 3. Internationalen Kongress „Sichere Identität“ in Berlin unter dem Titel „SumoDacs: Absicherung des mobilen Zugriffs auf Unternehmensanwendungen mit einer manipulationsresistenten Smartcard“ vorgestellt (siehe Zwischenbericht KIT). In dem Artikel wird zunächst die Grund-Architektur von SumoDacs mit den drei Zonen beschrieben. Dann wird erörtert, wie mit speziellen Security-Smartcards die Sicherheit des Gesamtsystems erhöht werden kann. Ein weiterer Teil des Artikels widmet sich der „Kontextabhängigen Zugriffskontrolle“.

*Modellierung von Ortseinschränkungen für mobile Geschäftsprozesse mit höheren Petri-Netzen*

Diese Veröffentlichung (siehe auch Zwischenbericht KIT) bezieht sich auf den Teilaspekt der Zugriffskontrollmodelle (AP 6). Im Beitrag wird ein Ansatz beschrieben, Einschränkungen für die zulässigen Ausführungsorte einzelner Prozessaktivitäten in mit höheren Petri-Netzen beschriebenen Prozessmodellen zu definieren. Diese sog. Ortseinschränkungen berücksichtigen auch prozessspezifische Merkmale, etwa dass innerhalb einer Prozessinstanz verschiedene Aktivitäten am selben Ort ausgeführt werden müssen.